United States Marshals Service POLICY DIRECTIVES

## INFORMATION RESOURCES MANAGEMENT

### 12.1 Information Resources and Technology Management

**A.** **Proponent:** Assistant Director for Information Technology Division (ITD) and Chief Information Officer (CIO). Telephone: 202-307-9677.

**B.** **Purpose:** To establish United States Marshals Service (USMS) policy governing the planning, management, operation, and use of information technology (IT) and information resources (IR). This policy applies to all persons who use USMS IT resources, including but not limited to employees, contractors, task force officers, and interns. This policy applies to classified and unclassified computer and telecommunications systems, technology, peripheral devices, and resources that are acquired for use by, owned, operated, or managed by USMS offices and users.

**C.** **Authority:** References to selected laws and regulations applicable to this policy directive are in Appendix 1, *Authority.*

**D.** **Policy:** ITD is responsible for the promulgation of policy, procedures, management and oversight, and provision of support services for all IR management and IT systems in the USMS. The Tactical Operations Division (TOD) is responsible for the management and provision of support services for secure telecommunications equipment and services.

1. The Assistant Director for ITD, also known as the CIO, is responsible for:

   a. Advising and assisting the Director, Deputy Director (DD), Associate Directors (AD), Assistant Directors (A/AD), United States Marshals (USM), and other senior USMS staff in order to ensure that the USMS plans, acquires, manages, and uses IT and IR in a manner that enhances mission accomplishment; improves work processes and paperwork reduction; provides sufficient protection for the privacy of personal information; promotes citizen-centered electronic government; and is consistent with all applicable federal laws and policy directives;

   b. Recommending USMS-wide policies, and issuing standards, procedures and guidelines to ensure an effective and integrated approach to IT planning, management, and reporting;

   c. Developing and managing a USMS IT Strategic Plan that supports Department of Justice (DOJ) and USMS mission-oriented goals and performance measures, and is consistent with the laws and regulations affecting IT security;

   d. Developing strategic performance measures which apply to the objectives in the DOJ IT Strategic Plan; and

   e. Developing, maintaining, and implementing the USMS Enterprise Architecture (EA) program. The EA program guides the selection and implementation of the USMS IT investments. The EA program:

1) Defines the various elements of USMS architecture, connections to departmental and federal architecture, and the interaction with other DOJ component architectures;

2) Delivers optimum IR requirements necessary to support DOJ's mission and strategic goals, thereby facilitating consolidated, centralized, and integrated component IT services which improve information access, quality, and economies of scale;

3) Identifies the IT capabilities required to achieve USMS IT strategic goals and specifies a plan to develop, acquire, and integrate those capabilities into DOJ's architecture;

4) Ensures compliance with the Office of Management and Budget (OMB) federal architecture guide, standards, and requirements; and

5) Ensures that USMS IT investments are aligned with DOJ architecture, and that those investments are delivering the expected technical and functional performance results.

f. Administering the IT Investment Management (ITIM) program. The CIO:

1) Establishes and maintains a USMS-wide enterprise portfolio management process that manages USMS investments from inception to retirement;

2) Integrates the USMS enterprise portfolio management process into the USMS budget process and manages the IT portion of the budget process; and

3) Ensures compliance with OMB federal investment management guidance and with DOJ and OMB reporting requirements.

g. Administering and coordinating USMS IT acquisition management with the Assistant Director for the Financial Services Division (FSD). The IT acquisition management process:

1) Is governed by the Federal Acquisition Regulations (FAR) and by the Justice Acquisition Regulations (JAR), Circulars, and Procurement Guidance Documents (PGD);

2) Includes the completion of key activities for acquiring products and services, including the identification of discrete units of work or modules to be contracted, market research, identification of competition, potential contracting sources, contract types and budget and funding;

3) Addresses risks and provides the appropriate incentives for contractors to perform based on the government's expectations;

4) Develops an acquisition strategy for all major IT projects, which shall be revised whenever significant changes occur during the life cycle of the IT project;

5) Utilizes acquisition planning to direct procurements throughout the life cycle of the major IT project;

6) Utilizes DOJ and General Services Administration (GSA) enterprise license agreements, if available, and adheres to OMB policy directives to procure products and services required for IT projects;

7) Utilizes modular contracting to acquire major IT systems to the maximum extent feasible to provide incremental benefits and costs versus lengthier contract delivery approaches. Contracts and modules shall be aligned with current and anticipated program funding. Contracts shall contain discrete units of work as identified in the acquisition strategy;

8) Utilizes Statements of Work (SOWs) which reference all of the relevant DOJ IT policies, the EA, and other standards including the Technical Reference Model (TRM), where compliance is required for the acquisition of IT products and services; and

9) Requires contractors to use an earned value management system to monitor and report on project cost and schedule performance outcomes.

h. Ensuring Privacy Impact Assessments (PIAs) are:

1) Conducted in accordance with the E-Government Act of 2002 and applicable DOJ and OMB guidance, including OMB Memorandum 03–22;

2) Conducted and reviewed prior to the development of a new system (or system modification), ideally when requirements are being analyzed and decisions are being made about data usage and system design; and

3) Published on a publicly available web site on a page devoted to privacy or to the system for which the PIA was conducted, or Freedom of Information Act (FOIA) electronic reading room.

i. Ensuring the compliance with and implementation of USMS-wide policy and procedures concerning the accessibility of DOJ information technology by federal employees, contractors, and members of the public sector, as specified by 1998 Amendment to Section 508 of the Rehabilitation Act.

j. Assessing IT human capital needs and requirements and developing and implementing strategies and plans for meeting these needs and requirements.

k. Reviewing and evaluating:

1) The performance of USMS IT programs and projects; and

2) IT funding requests, including reprogramming actions.

l. Providing IT services and operations to the USMS.

m. Delegating responsibilities, as necessary, for the effective and efficient operation of the USMS IR program and IT systems.

n. Consulting and coordinating, as appropriate, with the Office of General Counsel (OGC) to identify legal issues and ensure compliance with the E-Government Act of 2002, the Privacy Act of 1974, and other applicable statutes and regulations.

2. The Security Program Manager (SPM): The designation of a USMS security officer is intended to establish clear accountability for setting policy for all security matters, including personnel, physical, IT, and information security activities.
The SPM for the USMS is the Chief of the Office of Security Programs (OSP) within TOD.

**E. Procedures:**

1. All requests for waivers to this policy are to be submitted in writing, e-mail is acceptable, to the CIO, who will direct the request to the appropriate USMS official for approval.

2. Procedures associated with the management, use, allocation, deployment, and accountability of USMS IT resources and systems are found in Policy Directive 12.2, *The Management, Use, Allocation, Deployment, and Accountability of United States Marshals Service (USMS) Information Technology (IT) Resources and Systems*.

3. Procedures associated with USMS user accounts and IT system accesses are found in Policy Directive 12.3, *Information Technology Account Management and User Support*.

4. Procedures associated with the acquisition, management and use of network and telecommunications services and equipment are found in Policy Directive 12.4, *Guidelines for Telecommunications Requests*.

5. Procedures associated with ITIM, the IT strategic plan, and IT change management processes are found in Policy Directive 12.5, *Investment Management*.

6. Procedures associated with Intranet and Internet web management and E-Government are found in Policy Directive 12.6, *E-Government/Web Management*.

7. Procedures associated with IT security management are found in Policy Directive 12.7, *Information Technology (IT) Security*.

**F. Definitions:** References to selected terms and definitions applicable to this policy directive are in Appendix 2, *Definitions.*

***G.*** **Cancellation Clause:** Supersedes Policy Directive 12.1*, General Computer and Telecommunications Management*.

**H. Authorization and Date of Approval:**

| **By Order of:** | **Effective Date:** |
|---|---|
| /S/ | 3-19-2010 |
| John F. Clark<br>Director<br>U.S. Marshals Service | |

## 12.1 Information Resources and Technology Management
## Appendix 1: Authority

### 1. Congressional Mandates

a. Clinger Cohen Act of 1996 Pub. L. 104-106, Feb. 10, 1996, 110 Stat. 186; 4 USC 40001 et seq.; and, Pub. L. 104-208, Sept. 30, 1996, 110 Stat. 3009; 8 USC 808.
b. Computer Fraud and Abuse Act of 1986, 18 USC 1030 (1996).
c. Computer Security Act of 1987, Pub. L. 100-235, Jan. 8, 1988, 101 Stat. 1724; 15 USC 272, 278h, 278g-3, 278g-4, and 40 USC 759.
d. Federal Information Security Management Act of 2002 (FISMA), Pub. L 107-347, 44 USC 3541-3549.
e. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2511
f. Government Paperwork Elimination Act (GPEA); Pub. L. 105-277, Title XVII; USC 44 3504.
g. Workforce Investment Act of 1998, 29 USC 794d (Section 508 of the Rehabilitation Act of 1973), as amended.
h. E-Government Act of 2002, Pub.L. 107-347, 44 USC 35-36
i. Federal Managers Financial Integrity Act of 1982 (FMFIA), Pub. L. 97-255, 96 Stat. 814.
j. Freedom of Information Act (FOIA), 5 U.S.C. § 552.
k. Paperwork Reduction Act of 1995 (PRA), Pub. L. 104-13, 44 U.S.C. 3501-3520.
l. Privacy Act of 1974, 5 U.S.C. § 552a.

### 2. Federal Regulations/Guidance

a. 5 CFR 1320, Controlling Paperwork Burdens on the Public.
b. 28 CFR 45.4, Personal Use of Government Property.
c. 36 CFR 1194, Electronic and Information Technology Accessibility Standards (65 FR 80500, Dec. 21, 2000).
d. 41 C.F.R. 101-35, Telecommunications Management Policy.
e. Committee on National Security Systems Instruction (CNSSI) No. 7000, TEMPEST Countermeasures for Facilities.
f. CNSS Policy (CNSSP) No. 6, National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems.
g. CNSSI No. 4009, National Information Assurance Glossary.
h. CNSSI No. 4016, National Information Assurance Training Standard For Risk Analysts.
i. CNSS NSS Instruction 1199, Security Categorization for National Security Systems and Information (ODNI/CIO Draft).
j. CNSS NSS Instruction 1218, (ODNI/CIO Draft), Guide for Developing Security Plans for National Security Information Systems.
k. CNSS NSS Instruction 1230, (ODNI/CIO Draft), Risk Management Guide for National Security Information Technology Systems, provides guidance on the assessment and mitigation of risk as part of an overall risk management process.
l. CNSS NSS Instruction 1237, (Draft), Guide for the Security Certification and Accreditation of National Security Information Systems, provides guidance on the security authorization of NSSs.
m. CNSS NSS Instruction No. 1253, (ODNI/CIO Draft), Security Control Catalog for National 9 Security Systems.
n. CNSS NIST Special Publication (SP) 800-123, Guide to General Server Security: Recommendations of the National Institute of Standards and Technology.

### 3. Departmental Regulations/Guidance

a. Department of Justice (DOJ) 2421.1E, Use of Government Telecommunications Systems.
b. DOJ 2640.2F, Information Technology Security.

c. DOJ 2880.1B, Information Resources Management Program.
d. DOJ Order 2740.1A, Use and Monitoring of DOJ Computers and Computer Systems.
e. DOJ Order 2420.2, Telecommunications Policy and Guidelines.
f. USMS Directive 1.1 Delegation of Authority, Organization and Functions.
g. Personal Information on DOJ Web Sites, May 2, 2006.
h. DOJ Web Content Guidelines and Suggested Practices, May 10, 1999.
i. DOJ Information Technology, Security Staff (ITSS) Standards, as amended.
j. DOJ Order 2600.2C, Security Programs and Responsibilities.
k. DOJ Security Program Operating Manual (SPOM).
l. DOJ Order 2610.2A, Employment Security Regulations.
m. DOJ Certification & Accreditation Handbook, May 2009, as amended.

4. **Presidential and Executive Branch Guidance**

a. Executive Order 12958, Classified National Security Information, as amended.
b. EO 12968, Access to Classified Information.
c. EO 13231, Critical Infrastructure Protection in the Information Age.
d. EO 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans.
e. General Accounting Office (GAO) Federal Information System Control Audit Manual (FISCAM).
f. International Standard 15408, Common Criteria for Information Technology Security Evaluation.
g. Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection.
h. HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors.
i. National Security Directive 42, National Policy for the Security of National Security and Telecommunications and Information Systems.
j. National Security Presidential Directive (NSPD 51) / Homeland Security Presidential Directive (HSPD-20), National Continuity Policy.

5. **Office of Management and Budget (OMB) Guidance**

a. Office of Management and Budget (OMB) Circular A-127, Financial Management Systems.
b. OMB Memorandum 99-18, Privacy Policy on Federal Web Sites.
c. OMB Memorandum 00-13, Privacy Policies and Data Collection on Federal Web Sites.
d. OMB Memorandum 01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy.
e. OMB Memorandum 03–22, OMB Guidance for Implementing the Privacy Provisions of the E–Government Act of 2002.
f. OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies.
g. OMB Memorandum 04-26, Personal Use Policies and “File Sharing” Technology.
h. OMB Memorandum 05-02, Financial Management Systems.
i. OMB Memorandum 05-04, Policies for Federal Agency Web Sites, December 17, 2004.
j. OMB Memorandum 06-15, Safeguarding Personally Identifiable Information.
k. OMB Memorandum 06-16, Protection of Sensitive Agency Information.
l. OMB Memorandum 06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments.
m. OMB Memorandum 07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems.
n. OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.

o. OMB Memorandum 07-18, Ensuring New Acquisitions Include Common Security Configurations.
p. OMB Memorandum 07-24, Updated Principles for Risk Analysis.
q. OMB Memorandum 08-05, Implementation of Trusted Internet Connections (TIC).
r. OMB Memorandum 08-16, Guidance for Trusted Internet Connection Statement of Capability Form (SOC).
s. OMB Memorandum 08-22, Guidance on the Federal Desktop Core Configuration (FDCC).
t. OMB Memorandum 08-23, Securing the Federal Government's Domain Name System Infrastructure.
u. OMB Memorandum 08-27, Guidance for Trusted Internet Connection (TIC) Compliance.
v. OMB Memorandum 09-02, Information Technology Management Structure and Governance Framework.
w. Office of Management and Budget (OMB) Circular A-11, Preparation and Submission of Budget Estimates.
x. OMB Circular A-130, Management of Federal Information Resources (with Appendices and periodic revisions).
y. OMB Circular A-130 Appendix III, "Security of Federal Automated Information Systems."

6. **Other Applicable Agency Guidance**

a. National Institute of Standards and Technology (NIST) Recommended Security Controls for Federal Information Systems and Organizations,
b. NIST Special Publications 800-53, Recommended Security Controls, as amended:

1) 1.6 Classified Laptop and Standalone Computers, (Version 2.1), November 2006;
2) Access Control (Version 2.2), June 2008;
3) Audit and Accountability (Version 2.1) June 2008;
4) Awareness and Training (Version 3.1), dated June 2008;
5) Certification, Accreditation, and Security Assessments (Version 3.2), June 2008;
6) Configuration Management (Version 1.1), June 2008;
7) Contingency Planning (Version 2.1), June 2008;
8) Identification and Authentication (Version 2.1), June 2008;
9) Incident Response (Version 3.0), February 2009, Maintenance (Version 2.0), December 2006;
10) Media Protection (Version 3.1), June 2008;
11) Personnel Security (Version 3.1), June 2008;
12) Physical and Environmental Protection (Version 3.1), June 2008;
13) Planning (Version 3.2), June 2008;
14) Risk Assessment (Version 3.1), June 2008;
15) System and Communications Protection (Version 1.1), June 2008;
16) System and Information Integrity (Version 2.0), December 2006; and
17) System and Services Acquisition (Version 3.1), June 2008.

c. NIST Security Guidance, SP-800 series.

1) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, An Introduction to Computer Security: The NIST Handbook.
2) NIST SP 800-14, Generally Accepted Principles and Practices for Security Information Technology Systems.
3) NIST SP 800-16, Information Technology Security Training Requirements.
4) NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems.
5) NIST SP 800-27, Engineering Principles for Information Technology Security.
6) NIST SP 800-28, Guidelines on Active Content and Mobile Code.

7) NIST SP 800-30, Risk Management Guide for Information Technology Systems.
8) NIST SP 800-34, Contingency Planning Guide for Information Technology Systems.
9) NIST SP 800-35, Guide to Information Technology Security Services.
10) NIST SP 800-36, Guide to Selecting Information Technology Security Products.
11) NIST SP 800-37, Guide for the Security Certification and Accreditation for Federal Information Systems.
12) NIST SP 800-39, Managing Risk from Information Systems.
13) NIST SP 800-40, Creating a Patch and Vulnerability Management Program.
14) NIST SP 800-41, Guidelines on Firewalls and Firewall Policy.
15) NIST SP 800-44, Guidelines on Securing Public Web Servers.
16) NIST SP 800-45, Guidelines on Electronic Mail Security.
17) NIST SP 800-46, Security for Telecommuting and Broadband Communications.
18) NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems.
19) NIST SP 800-48, Guide to Securing Legacy IEEE 802.11 Wireless Networks.
20) NIST SP 800-50, Building an Information Technology Security Awareness and Training Program.
21) NIST SP 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations.
22) NIST SP 800-53, Recommended Security Controls for Information Systems.
23) NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems.
24) NIST SP 800-54, Border Gateway Protocol Security.
25) NIST SP 800-55, Security Metrics Guide for Information Technology Systems.
26) NIST SP 800-59, Guideline for Identifying an Information System as a National Security System.
27) NIST SP 800-60 (Vol. I and Vol. II), Guide for Mapping Type of Information and Information Systems to Security Categories.
28) NIST SP 800-61, Computer Security Incident Handling Guide.
29) NIST SP 800-63, Electronic Authentication Guideline.
30) NIST SP 800-64, Security Considerations in the Information System Development Life Cycle.
31) NIST SP 800-68, Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist.
32) NIST SP 800-70, Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers.
33) NIST SP 800-76, Biometric Data Specification for Personal Identity Verification.
34) NIST SP 800-77, Guide to IPsec VPNs.
35) NIST SP 800-81, Secure Domain Name System (DNS) Deployment Guide.
36) NIST SP 800-83, Guide to Malware Incident Prevention and Handling.
37) NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities.
38) NIST SP 800-88, Guidelines for Media Sanitization.
39) NIST SP 800-92, Guide to Computer Security Log Management.
40) NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS).
41) NIST DP 800-95, Guide to Secure Web Services.
42) NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.
43) NIST SP 800-100, Information Security Handbook: A Guide for Mangers.
44) NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices.
45) NIST SP 800-113, Guide to SSL VPNs.
46) NIST SP 800-114, User's Guide to Security External Devices for Telework and Remote Access.

47) NIST SP 800-115, Technical Guide to Information Security Testing and Assessment.
48) NIST SP 800-121, Guide to Bluetooth Security.
49) NIST SP 800-123, Guide to General Server Security.
50) NIST SP 800-124, Guidelines on Cell Phone and PDA Security.

d. NSA: NSTISSP No.101, National Policy on Securing Voice Communications, Dated September 14, 1999.
e. NSA: NTISSI No. 3013, Operational Security Doctrine for the STUBIII Type I Terminal, Dated February 8, 1990.
f. Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information Systems.
g. FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems.
h. FIPS Publication 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors.
i. Federal Continuity Directive 1 (FCD 1), Federal Executive Branch National Continuity Program and Requirements.
j. Intelligence Community Directive Number 503, Intelligence Community Information Technology Systems Security, Risk Management, Certification and Accreditation.
k. National Security Agency (NSA)/ Central Security Service (CSS) Policy 9-12, NSA/CSS Storage Device Declassification.
l. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 1000, National Information Assurance C&A Process (NIACAP).
m. National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products.
n. National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/2-95, RED/BLACK Installation Guidance.

**12.1** ***Information Resources and Technology Management***

**Appendix 2 - Definitions**

1. **Computer system and/ or telecommunications system** is a discrete set of electronic information resources (data, hardware and software) organized for the collection, processing, maintenance, transmission, and dissemination of information.

2. **Continuity of Operations Plan (COOP**) is document that establishes policies and procedures to provide for the continuance of critical IRM operations, that will ensure the continued performance of Departmental and component essential functions during any emergency or situation that may disrupt normal operations. The COOP must be in compliance with the Federal Emergency Management Agency's Federal Circular 65 and Order DOJ 2640.2E.

3. **Enterprise Architecture (EA)** is a blueprint that explains and guides how an organization's IT and information management elements work together to accomplish the mission of the organization. An EA addresses the following views: business activities and processes, data sets and information flows, applications and software, and technology. An EA includes a current (baseline) architecture, desired (target) architecture, and a sequencing plan.

4. **Information Resources,** as defined in Section 3502(6) of U.S.C. Title 44 [The Paperwork Reduction Act of 1995], refers to information and related resources, such as personnel, equipment, funds, and information technology. Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

5. **Information Technology (IT)** has the meaning given in Section 5002(3) of the Clinger-Cohen Act of 1996, which denotes any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. As further clarified in OMB Circular A-11, IT includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

6. **IT Contingency Plan (ITCP)** documents and maintains a plan for the continuity of general support systems and contingency plans for major applications. NIST Publication 800-34 considers continuity of support planning to be synonymous with IT contingency planning. OMB Circular A-130, Appendix III, and ITSS Standard 2.4 require the development and maintenance of ITCP's for every IT system and application. The general definition of the contingency plan is: "a plan used by an organization or business unit to respond to a specific systems failure or disruption of operations. A contingency plan may use any number of resources including workaround procedures, an alternate work area, a reciprocal agreement, or replacement resources."

7. **IT Investment** involves IT and information resources, including information or application system design, development, and maintenance, regardless of whether such work is performed by government employees or contracted out.

8. **IT Investment Plan** identifies the investments (for projects and programs) sought to implement the EA and specifies the priority of the investments in relation to mission criticality and management visibility, as well as information concerning investment sequencing and other dependencies to guide planners during project selection.

9. **IT Project Manager** manages the day-to-day project activities. In the case where an investment is for one project, the IT and investment project managers are one and the same. In the case where an investment is for multiple projects, the IT project manager and investment project manager may be different people.

10. **IT Security Controls.** Security controls are the organizational safeguards and counter measures that provide specific protections for IT systems, system users, and the information contained in IT systems. Security controls are the management, operational, and technical safeguards or counter measures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Appropriate security controls provide reasonable assurance in mitigating the risk incurred by the use of information and information systems in the execution of organizational missions and business functions.

11. **Internet** is the publicly available worldwide network of computer systems, services and electronic media, interconnected through the Transmission Control Protocol/Internet Protocol, and related protocols.

12. **Intranet** is any private, or limited access network of computer systems, services and electronic media, interconnected through the Transmission Control Protocol/Internet Protocol, and related protocols.

13. **Investment Project Manager** oversees the whole investment. In the case where an investment is for one project, the investment and IT project manager are one and the same. In the case where an investment is for multiple projects, the investment manager and IT project managers may be different people.

14. **Major IT Investment** is a system or investment that requires special management attention because of its importance to an agency's mission; a major investment in the prior year's budget submission and is continuing; an investment for financial management and spends more than $500,000; an investment directly tied to the top two layers of the Federal Enterprise Architecture (Services to Citizens and Mode of Delivery); an investment that is an integral part of the agency's modernization blueprint (EA); an investment that has significant program or policy implications; an investment that has high executive visibility; or an investment defined as major by the agency's capital planning and investment control process. Investments that are E-Government in nature or use e-business technologies must be identified as major investments regardless of the costs. Systems not considered "major" are "non-major."

15. **Major information system** embraces “large” and “sensitive” information systems and means, as defined in OMB Circular A-130 (Section 6.u.) and annually in OMB Circular A-11 (section 300-4 (2003)), a system or project that requires special management attention because of its: (i) importance to the agency mission, (ii) high development, operating and maintenance costs, (iii) high risk, (iv) high return, (v) significant role in the administration of an agency’s programs, finances, property or other resources.

16. **Personal digital assistant (PDA):** A handheld device (e.g., tablet computer, notebook computer, palm-type computer) that includes or combines computing, telephone/fax, email and networking features.

17. **Portable remote computing devices:** Mobile IT systems that denote laptop computers, PDAs, pagers, Blackberries, cellular phones, and other portable devices that are capable of storing and transmitting information.

18. **Portfolio** is a collection of IT investments necessary to achieve strategic goals and accomplish mission and program objectives.

19. **Privacy Impact Assessment (PIA)** is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

20. **Remote Access** is any access to a USMS's nonpublic information system by a user (or an information system) communicating through an external, non-Department-controlled network (e.g., the Internet) using a USMS controlled computer.

21. **Sensitive and Personally Identifiable Information (PII)** The term "personally identifiable information" refers to information that can be used to distinguish or trace individuals' identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. The loss or disclosure of sensitive information not only has a serious negative impact on law enforcement and other critical functions, but also diminishes the public trust in law enforcement operations. There is inherent risk in carrying such data on mobile computers and devices.

22. **Systems Development Life Cycle (SDLC**) is the period of time from when a system is first conceived (concept development) to when the system is no longer available for use (disposition or retirement).

23. **Users**: Individuals who are authorized to use USMS information systems. Users include USMS employees (including ITS staff), contractors, and others who have undergone a favorably adjudicated background investigation by the USMS or who have been granted extra-DOJ access (e.g., through a Memorandum of Understanding or via RISSNET/LEO) to access and use USMS computer and telecommunications systems.

United States Marshals Service POLICY DIRECTIVES

## INFORMATION RESOURCES MANAGEMENT

### 12.2 The Management, Use, Allocation, Deployment, and Accountability of United States Marshals Service (USMS) Information Technology (IT) Resources and Systems

**A. Proponent:** Chief Information Officer (CIO), Assistant Director for Information Technology, and the Information Technology Division (ITD). Telephone: 202-307-5200.

**B. Purpose:** To provide policy directive and guidance to all elements of the United States Marshals Service (USMS) for the allocation, deployment, and accountability of computer and telecommunications resources on a nationwide basis. This policy directive applies to all classified and unclassified computer resources systems and peripheral devices that are acquired for use by, owned, operated, or managed by the USMS.

**C. Authority:** Department of Justice (DOJ) Order 2880.1B, *Information Resource Management Program*; DOJ Order 2640.2F, *Information Technology Security*; DOJ Order 2420.2, *Telecommunications Policy and Guidelines*; DOJ Order 2740.1A, *Use and Monitoring of DOJ Computers and Computer Systems*; DOJ 2421.1E, *Use of Government Telecommunications Systems*; USMS Policy Directive 1.1, *Delegation of Authority, Organization and Functio*ns; Office of Management and Budget (OMB) Memorandum M-08-05, *Implementation of Trusted Internet Connections (TIC)*.

**D. Policy:**

1. **Authorized Use of USMS Computer and Telecommunications Resources and Systems:**

   a. **General:** Use of USMS computer and telecommunications systems, including desktop phones, cell phones, pagers, desktop computers, portable remote computing systems (including laptops and hand-held devices), e-mail, word processing systems, and connections to Internet or Intranet sites, is subject to the same restrictions on use as are other government-furnished resources provided for the use of employees.

   b. **Personal Use:** While USMS computer and telecommunications systems are provided for official use, some personal use of government computer and telecommunications systems is permitted in accordance with existing policy directive on personal use of government property, where there is negligible cost to the government and no interference with official business. Supervisors may deny employees access to information technology (IT) systems or the Internet, and employees may be disciplined up to and including removal for inordinate or inappropriate personal use of USMS computer and telecommunications systems (reference: DOJ Order 2740.1a Sections 3 c and d).

   c. **USMS-Provided Information Technology Resources:** Only USMS-provided computer and telecommunications systems may be used to perform official

USMS work; and only USMS-provided computer and telecommunications systems may be connected to USMS networks. Personally owned systems, systems used by contractors, systems from other federal, state, or local agencies, and any non-USMS controlled systems are not authorized for connectivity to the USMS network and other IT resources. Exceptions to this Departmental and USMS policy must be requested through and approved by the CIO.

d. **Portable Devices:** The normal execution of the USMS mission necessitates the use of portable remote computer systems such as laptop computers, notebook computers, hand-held computer devices, tablet computers, paging devices, and cellular communication devices. The inherent wireless, mobile nature of portable remote computing systems presents unique, universally present security risks which threaten security of the devices themselves, the systems they access, and the data contained on them. Special precautions must be followed to protect all information related to portable remote computing systems to ensure the uniform, secure, uninterrupted execution of the mission of the USMS and to ensure the integrity and security of the USMS. Supervisors and employees must carefully weigh the dangers of potential loss or disclosure of sensitive information against the convenience of portable computing and take prudent measures to protect the devices, accessed systems, and data on them.

e. **The Use of Electronic Mail (e-mail) for Official Business:** All e-mail messages must contain sufficient information to identify the USMS individual and the office he or she represents, as well as minimal amount of contact information to facilitate further communication via various methods, for example, by telephone, facsimile and postal mail.

1) **Official E-Mail Address:** USMS staff will utilize a usdoj.gov e-mail address for official e-mail correspondence. The e-mail address can either be an individual staff member address or an authorized address associated with a specific mission based function (e.g. helpdesk@usdoj.gov).

2) **E-mail Signature Blocks:** E-mail signatures are a representation of USMS and should be professional in nature. E-mail signatures can be utilized to provide information about the author of an e-mail: name, contact and organizational information, address, mobile or fax numbers, and e-mail disclaimers. If the disclaimer is longer than two lines, consideration should be given to placing the disclaimer at the bottom of an e-mail message.

a) E-mail disclaimers should not extend beyond ten lines. Refer to Section F, Definitions, on e-mail disclaimers and Policy Directive 17.6.3, *Document Security* for additional guidance.

b) Quotations that are not directly mission related are prohibited.

c) Images are not authorized in signature blocks.

d) Signature blocks should be displayed as plain text in a fixed-width 8 to 12 point font (no HTML, web, or other rich formatted text).

3) **Use of E-mail Stationery:** The use of e-mail stationery or background images for official correspondence is not authorized.

2. **Prohibited Use of USMS Computer and Telecommunications Systems:** Certain activities are prohibited on USMS computer or telecommunications systems, during working or non-working hours, except when conducting legitimate USMS business, without prior express approval of the authorized official. Prohibited activity may lead to disciplinary action up to and including removal.

a. **Prohibited Activities:**

1) Use of Internet sites that result in an additional charge to the government;

2) Obtaining, viewing, or transmitting sexually explicit material or other material inappropriate to the workplace. The exception to this prohibition is an authorized activity associated with criminal investigations based on the Adam Walsh Child Protection and Safety Act of 2006 and violations of 18 USC 2250;

3) Use of USMS computer or telecommunications systems for other than official government business that results in significant strain on the systems (e.g., mass mailings; sending or downloading large files such as programs, pictures, video or music files, or games);

4) Any otherwise prohibited activity, such as sending out solicitations or engaging in political activity prohibited by the Hatch Act;

5) Using government office equipment for activities that are illegal, inappropriate, or offensive to government staff or the public. Such activities include hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation;

6) Any use of software or hardware to circumvent security controls on DOJ or other external IT systems; and

7) Use of IT resources or property for commercial purposes, or in support of "for-profit" activities, or in support of other outside employment or business activity (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services).

b. **Authorizing Official for Prohibited Activities:** Prior written approval by the CIO or Deputy Assistant Director for ITD is required for USMS employees to engage in otherwise prohibited USMS computer, or telecommunications system activities for official duty purposes such as USMS investigations, or use of prohibited software or hardware.

. For IT activities specifically associated with criminal investigations based on the Adam Walsh Child Protection and Safety Act of 2006 and violations of 18 U.S.C. § 2250:

1) The CIO is responsible for providing general network and IT authorizations to access prohibited web Internet content and exemptions from prohibited IT activities specified in 12.2.D.2.

2) Supervisory Deputy United States Marshals (SDUSM) are responsible for granting written prior permission to engage in the prohibited activities specified in 12.2.D.2.a.2 for open criminal investigations. Participation in the prohibited activity can only be authorized in connection with and to further an open USMS investigation in which the requesting Deputy United States Marshal (DUSM) is involved.

3) DUSMs engaged in ongoing criminal investigations are responsible for obtaining authorization and documenting specific instances of IT related activity associated with investigative activities in investigative reports as specified in 12.2.E.2.

3. **Monitoring of Computer and Telecommunications Systems:** The use of a USMS computer or telecommunications system, including a personal computer connected to the USMS or DOJ network, constitutes consent to monitoring. The USMS monitors employee Internet and other computer/telecommunications system activity to ensure that the requirements in this directive are not violated. The USMS authorized officials may monitor and access e-mail or voice mail messages, Internet activities, documents, files, or other information on government computer/telecommunications systems whenever there is a legitimate governmental purpose for doing so.

a. **Authorizing Officials:** Monitoring and accessing employees' e-mail or voice mail messages, Internet activities, documents, files, or other use of USMS computer or telecommunications systems may be only for authorized purposes. Access to an employee's computer or telecommunications system for any reason except those specified below, such as for suspected misconduct not connected with an official investigation, must be authorized by the Director or Deputy Director of the USMS. The CIO will be the point of contact for all such access requests.

b. **Authorized Purposes for System Monitoring or Access include:**

1) For system administration and system security;

2) For conduct of an official investigation by USMS Office of Internal Investigations (OII), the Office of Professional Responsibility (OPR), District / Division investigation, the Office of the Inspector General (OIG), the Federal Bureau of Investigation (FBI), or the Criminal Division; and

4) For response to a court order, grand jury subpoena, or search warrant.

c. **Web Usage:**

1) All web access shall be conducted through the USMS and the DOJ enterprise web access resources. Any waivers to this requirement must be submitted in writing to the CIO, who will seek DOJ approval as appropriate. Waiver requests are to be made before implementation of alternative web access.

2) To maximize network efficiency and conserve bandwidth, web browsers should be turned off when not being actively used.

d. **Unauthorized System Use, Access or Monitoring:** Nothing in this policy directive creates any enforceable rights; however, unauthorized use, monitoring of, or improper attempts to access an employee's computer or telecommunications system may result in disciplinary action up to and including removal, and / or loss of computer or telecommunications system privileges.

1) Employees are prohibited from accessing the e-mail, electronic files or documents, or otherwise monitoring the online activities of another employee except in accordance with this guidance.

2) Accessing shared storage (i.e., a public or a shared server disk drive) does not constitute accessing another employee's computer or telecommunications system.

3) **Violations:** Any employee who uses an official government workstation for purposes other than those as authorized in this policy directive may be subject to disciplinary action up to and including removal of the employee from the USMS.

4. **User Responsibilities:** Safeguarding computer and telecommunications systems, computers and other devices is the responsibility of the person to whom they are assigned.

a. All USMS data/files must be backed up on a regular, recurrent basis. The CIO and delegated IT staff are responsible for maintaining backup procedures and capabilities. IT users are responsible for ensuring workstations are accessible for completing backup procedures.

b. Computers, mobile devices and telecommunications systems are not to leave the personal control of the person to whom they are assigned. If for any reason they must be left unattended, they should be secured in a manner that will protect the device from a potential threat (locked in car trunk, locked in home, locked in office, locked in security locker, etc.).

c. USMS computer and telecommunications systems are intended for exclusive use by the USMS and may not be utilized by non-USMS employees (family, task force personnel, visiting law enforcement officers, etc.) unless approved in writing by the CIO or Deputy Assistant Director for ITD.

d. Users must immediately notify their superiors and ITD Helpdesk or ITD Security of any suspected breach of security.

e. USMS mobile computers and hand-held devices are required to have approved agency encryption deployed when outside of DOJ/USMS auspices.

5. **Accountable Property Considerations:** Consistent with Policy Directive 7.1, *Management of Personal Property,* as accountable property, all automated data processing equipment (also known as IT equipment) having data storage capability (memory), computers (laptop, desktop, other), computer servers, removable (high security) hard disk or flash drives, and personal digital assistants (PDAs), BlackBerry devices, Global Positioning System equipment (GPS), and digital cameras are accounted for through the use of Form USM-325, *Hand Receipt*.

a. Form USM-325, *Hand Receipt*, is used to record and control accountable IT property issued to employees and all property on loan to another

organization. IT accountable property is defined in Policy Directive 7.1, Appendix A, *Forms.*

b. IT accountable property not issued to employees (e.g., computers assigned to a squad room or cell block area), must be controlled by use of hand receipt and maintained by the office's Property Custodian or their designee who has control over the specific IT property.

c. New IT equipment will be properly documented in the USMS property management system by ITD. The equipment and associated Form USM-325, *Hand Receipt*, will be forwarded to the intended office and individual to whom the IT equipment was assigned.

d. Identification of Official Government Workstations: Official government workstations used for investigative, law enforcement, or intelligence duties are not required to display official United States Government identification – FPMR, section 101-38.200 (f)]. Otherwise, all government workstations should be marked with appropriate labels to identify the level of information that may be processed on the workstation. For hand-held devices such as BlackBerrys or radios, the accountable property tags can be placed inside of the battery compartments. Memory devices such as approved flash drives, that are smaller than the appropriate labels, are exempt from the requirement of affixing USMS or government labels.

e. IT accountable property is not to be given, loaned, or otherwise transferred to another USMS IT user without first obtaining a signed hand receipt and delivering a copy to the appropriate property custodian. Users shall notify the property custodian immediately when the computer or telecommunications system has been reassigned, lost, or disposed of so that the USMS accountable property inventory can be kept accurate and current.

f. Any computer equipment to be disposed of, regardless of the disposal method, that has a hard drive or flash based memory or memory chips is to be "wiped" or degaussed in a manner prescribed by ITD. Media that is intended to be discarded should be done in accordance with USMS ITD disposal guidelines. Form OBD-239, *Equipment/Safe Inspection Certificate*, should be completed for wiping and degaussing IT equipment.

6. **Standard IT Workstation Configurations:** The USMS has established standard hardware and software configurations for classified and non-classified official computer workstations which cannot be deviated from without express, written authorization from the CIO or designated delegated ITD official. Any deviations to these standards must be approved by ITD prior to procurement (through ITD sign-off on USMS requisition documents). Unauthorized deviations to the standards will not be supported by ITD and will not be allowed on the USMS infrastructure. Standards for Workstation Configurations can be found at: http://web.usms.gov/most/hardware/. Software standards can be found at http://web.usms.gov/most/software/.

a. As a participant in the DOJ Consolidated Office Network (JCON) program, the USMS must comply with the standard JCON architecture. No hardware/software other than the standard configuration may be connected to the USMS network without express, written authorization from the CIO. Failure to comply with the JCON standard architecture can cause significant technical support problems and security vulnerabilities and will result in an immediate disconnect from the USMS network.

b. Systems directly connected to the USMS network within USMS controlled office space cannot have any modem or Wi-Fi active while on the network unless expressly authorized by the CIO, the Deputy Assistant Director for ITD, or a designated official that directly reports to the Deputy Assistant Director for ITD. USMS systems (e.g., desktops, laptops, portable computing devices) may only be used to connect to the USMS network; direct communications to other networks (e.g., Internet) are not allowed.

c. USMS systems may be connected to the USMS network through remote access (e.g. working from home, official travel, remote locations) under the following conditions:

1) Remote access systems shall be restricted to government-owned or contractor-owned systems;

2) Remote access from personally owned or "public computers" is prohibited;

3) Remote computers shall employ anti-viral software, firewalls, and encryption of stored data using FIPS 140-2 validated or NSA approved encryption;

4) Remote computers shall have all current and applicable Operating System (OS) and application security updates in place. The user shall ensure that the remote access computers have USMS approved security software in place, the OS is fully patched, antivirus software is installed and up-to-date, and a personal firewall is enabled;

5) Remote access computers shall use two-factor authentication where one factor is provided by a device separate from the computer gaining access;

6) Remote access computers shall use an encrypted Virtual Private Network (VPN) to connect to Department information systems;

7) Remote access computers shall not be connected to any other network when connected to a USMS or Departmental IT system; and

8) Remote access login sessions shall be restricted to a single operating system and a single network interface card when connected to a USMS IT system.

d. Configuration changes (including loading of software that is not included on the standard image) shall be approved by the CIO or designated ITD official, and be made only by ITD staff. Prior to implementation of any configuration changes, testing shall be performed by ITD to ensure incompatibilities or security risks are not introduced to USMS systems.

e. Untested software or software from unknown sources is not allowed on USMS computers or telecommunications systems. All software will be kept up-to-date with the most current, approved version of software.

f. Virus protection software adopted by ITD will be loaded on each computer system.

g. Systems with Solaris, Linux, and Unix operating systems may remain on the USMS network only if they are maintained with the most recent operating system and patches.

h. Unless authorized by the CIO or designated IT official for mission related requirements, anonymizer sites or hardware (anonymizer sites hide the user's identity from the Internet site being visited) are prohibited for use.

i. USMS workstations or laptops that have been off line or not directly connected to the USMS network, and have not been powered on for more than 30 days, should not be reconnected to the USMS network until the machines can be manually scanned to ensure anti-virus and other software patches are current.

j. **Restrictions on the use of Wi-Fi Systems:**

1) **Network Usage:** Wi-Fi technology is not authorized for use within the USMS Network (MNET). No wireless access points or wireless adapters may be connected to USMS IT equipment that is also directly connected to the MNET;

2) USMS personnel will not simultaneously use a Wi-Fi connection and have an established wired connection to any DOJ/USMS network environment (e.g., users shall not connect laptops onto DOJ/USMS networks without disabling air cards and/or internal wireless cards first);

3) USMS personnel using Wi-Fi resources shall use an approved Justice Secure Remote Access (JSRA) token whenever practical;

4) USMS personnel using Wi-Fi resources are prohibited from connecting to any information system that processes classified information;

5) Use of USMS Wi-Fi resources is intended for authorized personnel and official USMS business;

6) USMS personnel using Wi-Fi resources shall adhere to the DOJ Rules of Behavior (ROB);

7) USMS personnel using Wi-Fi resources shall ensure that anti-virus software and operating system patching is up-to-date; and

8) Exceptions: Any exceptions or waivers to the Wi-Fi policy must be granted in writing by the Assistant Director, ITD, or the Deputy Assistant Director, ITD. Exceptions may be granted on a temporary basis in exigent or contingency circumstances.

k. **Authorized use of Wi-Fi Resources:** Wi-Fi access to USMS non-classified information and information systems can be utilized with the use of an approved JSRA token via an encrypted connection in the following situations:

1) Working from home: When feasible, USMS laptops or desk tops that are utilized in a home setting should be directly connected to a router or modem. See guidelines for home use;

2) Working on a laptop while traveling and accessing USMS information systems in an airport or lodging accommodations;

3) Working in a non-USMS office setting while conducting official business;

4) Working in mission-based operational conditions outside of an office environment; and

5) Working in a USMS office setting where network connectivity is not available or is being repaired.

7. **Non-standard IT Workstation Configurations:** IT computer workstations that are not configured according to JCON configuration standards may be used for USMS mission based activities as stand-alone devices unconnected to the MNET. ITD is responsible for maintaining information and general guidelines on approved software and hardware for non-standard IT workstations.

a. Non-standard IT workstations and their configuration must be authorized by the CIO, or by authorized ITD officials as delegated by the CIO.

b. Pending the completion of technological solutions in the configuration, centralization, and implementation of a DOJ Trusted Internet Connection (TIC) for operational Internet activities, non-standard IT workstations can be connected to the Internet through commercial digital subscriber line (DSL) or cable connections if and only if the workstation configurations and security configurations of the Internet connections are reviewed and authorized by ITD. Written authorization to establish a DSL or cable connection for mission based activities must be obtained from the CIO, or from an IT official as delegated by the CIO.

c. Non-standard IT workstations will have authorized firewall and intrusion protection software, virus protection and anti-spyware software, a non-DOJ web browser, and data encryption software properly configured on the workstation.

.

d. Non-standard IT workstations will be configured to ensure data and information is protected against loss or theft, commensurate with security standards associated with the nature and type of information that is maintained on the workstation.

e. Users of non-standard IT workstations are responsible for ensuring that appropriate internal controls and IT data management processes are utilized to guarantee that data and information used for investigative reports are clear of intrusion tools, infections, and viruses.

8. **Acquisition of IT Hardware, Software and Services:** The USMS acquires IT hardware and software to fulfill USMS mission requirements from a variety of methods and sources. It is critical that the agency manage IT hardware and software inventory across the USMS from an enterprise perspective to ensure accountability, efficiencies of cost, security of software, and baseline and customer support of platforms.

a. **Authority:** The CIO, or ITD officials as delegated by the CIO, is responsible for all IT purchases, regardless of dollar value. Delegation of procurement authority for IT equipment and software is determined by the CIO.

b. **Funding for USMS IT Hardware, Software, Telecommunications Services and Equipment:** IT purchases are controlled and managed by the CIO and ITD. Funding for IT equipment, software, and services are made from the ITD

base allocation, or from funds transferred to the ITD work plan. When a procurement action cannot be initiated and completed by ITD, the purchase must be approved by ITD before the acquisition is made as set forth in accordance with Policy Directive 6.2, *Acquisition Processing, Section 3.b*.

c. **Capital Equipment Replacement Plan (CERP):** The Capital Equipment Replacement Plan (CERP) establishes the basis for determining agency funding requirements for the allocation and lifecycle replacement of all capital IT equipment. The quantity of equipment to be purchased through the CERP program will be based on the allocation formula for equipment in Section 9 of this policy. All CERP purchases will be made by ITD, through USMS or other authorized Federal acquisition vehicles.

1) **Acquisition of Individual Replacement Items:** In the event mission-critical equipment breaks down during a time period when the affected office is not eligible for CERP lifecycle replacement funding, ITD will review the requirements to determine the most efficient course of action for the replacement of the IT equipment.

2) **Acquisition of Items for New Mission Requirements:** In the event a new program is initiated, a new office is required to be opened, or a new technological solution for a USMS mission is identified, ITD will purchase the IT resources needed to meet the new requirements. When the new program or new office is provided funding as part of its start up, the IT funding will be transferred to ITD for the acquisition of the necessary IT resources.

d. **Requests for IT Resources:** A division or district requiring additional IT hardware, software, or services must submit the request and the stated requirements to ITD.

e. Purchases of hardware or software that do not conform to current USMS IT standards must be tested and authorized through the ITD Request for Change (RFC) process.

f. For short-term leases of IT equipment to meet specific operational needs, local leases may be authorized. Written approval from ITD is required prior to negotiating local leases for IT equipment.

g. **Wireless Consolidation Strategic Sourcing:** In concert with the USMS Chief Procurement Officer, to maximize cost effectiveness and operational efficiency, division and district offices are required to utilize Blanket Purchase Agreements that have been established for the use of BlackBerry mobile devices. Specific procedures are outlined for the Strategically Sourced Wireless Services on the ITD web page.

h. **IT Services Contracts:** All IT related services contracts require the review and authorization of the CIO, or ITD official as delegated by the CIO.

i. The purchase of printers, facsimile machines, and other multifunction output devices require the approval of the CIO or ITD officials as delegated by the CIO. The management and procurement of networked copy machines are the responsibility of the Assistant Director, Management Services Division

(MSD). The CIO is responsible for the network configuration of network copy machines.

9. **IT Workstation Allocations:** In general, one IT workstation will be allocated for each USMS employee. The exceptions to this ratio pertain to division or district management positions, staff assigned to classified operations, and specific mission based operational activities.

   a. Consistent with IT security and property management standards, DUSMs will be assigned one laptop which will follow them through various assigned positions (e.g., lateral transfers between district offices, promotions). New district positions will receive new laptops assigned to the specific budgeted position.

   b. **District Workstation Allocation Formula:** The formula for determining the current number of workstations for a district office is outlined below. Deviations from this allocation formula must be requested and documented in writing to the CIO.

| **Recommended Workstation Allocation Formula – District Offices** | | | |
|---|---|---|---|
| **Positions** | **Desktop** | **Laptop** | **Comments** |
| United States Marshal (USM) | 1 AND/OR | 1 | Incumbents of these positions can elect to have one laptop or desktop, or both types of computers. |
| Chief Deputy United States Marshal (CDUSM) | 1 | 1 | |
| Assistant Chief Deputy United States Marshal (ACDUSM) | 1 OR | 1 | Incumbents of these positions can elect to have either one laptop or one desktop. |
| SDUSM | 1 OR | 1 | |
| Task Force Member (USMS Employees) (Based on Public Law or HQ/AD Approval) | | 1 | Incumbents of these positions will be assigned laptops that will follow them to various assignments. |
| Criminal Investigators | | 1 | |
| DUSMs | | 1 | |
| Other Law Enforcement | 1 | | For security and accountability of equipment, non-USMS staff will be limited to conducting official business on USMS workstations within USMS controlled space. |
| Administrative Officer | 1 OR | 1 | Incumbents of this position can elect to have either one laptop or desktop. |
| Administrative Staff | 1 OR | 1 | District management can determine whether to assign one desktop or one laptop to administrative staff. |
| Interns | 1 | | For security and accountability of equipment, interns will be limited to desktop computers. |

| Recommended Workstation Allocation Formula – District Offices | | | |
|---|---|---|---|
| Contract Staff (Administrative Functions) | 1 OR | 1 | District management can determine whether to assign one desktop or one laptop. Funding for the workstation is to be provided by the program area managing the contract. |
| Contract Staff (Guard Functions) | 1 | | One desktop computer for a supervisory guard position (not for each guard). |
| Squad room or general use | 1 | | District management can elect to have a number of desktop computers for general use. The number of general use desktop computers should not be greater than 10 percent of the number of operational staff located in the specific district office or sub-office. |
| Task Force Members (Other Agencies) | 1 OR | 1 | For security and accountability of equipment, non-USMS staff will be limited to conducting official business on USMS workstations within USMS controlled space. Funding for the workstation is to be provided through the task force funding source |

c. **Division Workstation Allocation Formula:** The formula for determining the current number of workstations for a division office is outlined below. Deviations from this allocation formula must be requested in writing to the CIO.

| Recommended Workstation Allocation Formula – Division Office | | | |
|---|---|---|---|
| **Positions** | **Desktop** | **Laptop** | **Comments** |
| Assistant Director | 1<br>AND/OR | 1 | Incumbents of these positions can elect to have one laptop or desktop, or both types of computers. |
| Deputy Assistant Director | 1 | 1 | |
| Branch Chiefs, Chiefs | | 1 | Incumbents of these positions will be assigned laptops that will follow them to various assignments. |
| Assistant Chiefs, Supervisors | | 1 | |
| Division Staff – Analyst/Specialist/ Investigator levels | 1 OR | 1 | Division management can determine whether to assign one desktop or one laptop to administrative staff. |
| Division Staff - Clerical Support levels | 1 | | For security and accountability of equipment, one desktop computer for clerical support positions. |

| Recommended Workstation Allocation Formula – Division Office | | | |
|---|---|---|---|
| Contract Staff (Administrative Functions) | 1 OR | 1 | Depending on the nature of the work, Division management can determine whether to assign one desktop or one laptop to administrative staff. |
| Interns | 1 | | One desktop computer for an intern position. |
| Contract Staff (Guard Functions) | 1 | | One desktop computer for a supervisory guard position (not for each guard). |
| Squad room or general use | 1 | | District management can elect to have a number of desktop computers for general use. The number of general use desktop computers should not be greater than 10 percent of the number of operational staff located in the specific division office. |

10. **Portable Telephones, Personal Digital Assistants (PDAs), Smart Phones:** With the exception of radios, ITD is responsible for the administration of all wireless devices and systems, both on and off the USMS network. The USMS has limited and standardized the use of hand-held portable devices to BlackBerry mobile devices. All other types and forms of PDAs are not authorized for use on the MNET. Refer to USMS Directive 12.4 for additional guidance and allocation policy for mobile devices.

    a. **Wireless Consolidation Strategic Sourcing:** BlackBerry mobile devices will be obtained through the centralized procurement agreements established by ITD and the Financial Services Division (FSD). See section D.8.d.

    b. The Wireless Services Board is responsible for the adjudication of the wireless program, including the consideration of new devices and services. Members of the Board are appointed by the CIO.

    c. Requests to approve alternative goods, services, and/or devices through existing procurement vehicles established by ITD and FSD should be submitted through the Wireless Services Board. In order for a device or service to be included in the existing procurement contracts, an extensive technical and price performance evaluation will be completed, the Board will review, and contract modifications may be issued, as required. The Board will only consider changes that provide a substantial benefit to USMS missions, over and above current offerings, and at a cost benefit to the USMS.

    d. Employees are not authorized to make changes to the goods, devices or services available through the existing contracts. Also, absent specific authority and approval granted by the Wireless Services Board, employees are not authorized to expend government funds to purchase wireless devices, good, and/or services outside of the authorized contracts.

11. **IT Printers:** Workstation and office printers are managed through a centralized process to ensure accountability of equipment and to obtain efficiencies relating to the cost for supplies and services. Division and district offices should reduce the number of individual workstation printers or output devices through the use of network devices and multifunction printers that match the needs for each office.

a. District and division offices should have the capability to document workload statistics on the following characteristics to document specific printer needs: type of printing (color or black and white); range of output (print only, scan, copy, fax); anticipated printed page output (number of pages per month); range of paper sizes (4x6 in, 8.5x11, 8.5x14, 11x17); operating systems (Windows, Macintosh); network connections, paper handling (one sided printing, two sided printing, additional paper trays, stapling/ stacking); and input capabilities (auto-feed, flat bed, e-mail scanning).

b. To reduce costs and increase the effectiveness of managing printers, ITD is responsible for maintaining a standardized list of approved IT printing equipment, as well as for establishing procurement vehicles for acquiring printers. A list of authorized printers is located on the ITD web page. The Publishing and Multimedia Services Office (PMSO), MSD, also provides centralized management of multifunction network copiers.

c. **Recommended division office printer ratios:**

| **Recommended Printer Ratio Allocation for Division Offices** | |
|---|---|
| Type of Printer | Position or Office |
| Individual Printer | For each Assistant Director, Deputy Assistant Director, Branch Chief, Chief, Assistant Chief, Administrative Officer, Supervisor |
| Network printer | One printer for 20 workstations |
| Scanners | One scanner for every 20 workstations |
| Mobile printers | One mobile printer for every 8 laptops |

d. **Recommended district office printer ratios:**

| **Recommended Printer Ratio Allocation for District Offices** | |
|---|---|
| Type of Printer | Position or Office |
| Individual Printer | For each USM, CDUSM, ACDUSM, Administrative Officer, and Supervisor |
| Network printer | One printer for 20 workstations |
| Scanners | One scanner for every 20 workstations |
| Mobile printers | One mobile printer for every 8 laptops |

**E. Procedures:**

1. **Authorization to Use IT Resources in IT Prohibited Activities:** Written requests are submitted through appropriate chains of command to the CIO or Deputy Assistant Director for ITD. Written requests will be coordinated by the CIO and submitted to DOJ or other filtering entity for action. Specific written requests should contain information for each employee, the specific web sites, and the reason for requiring access. USMs may delegate their authority to submit requests to access restricted web sites to CDUSMs.

2. **Authorization for Obtaining, Viewing, or Transmitting Sexually Explicit Material or Other Material for Open Investigations Associated with the** Adam Walsh Child Protection and Safety Act of 2006 **and violations of** 18 U.S.C. § 2250**:**

a. Prior to engaging in the prohibited activity, the authorization should be described on a Form USM-11, *Report of Investigation*, that includes in its narrative portion

the specific prohibited activity for which authorization is sought; a brief explanation of how access to the prohibited activity is expected to advance the investigation; and the date and time the supervisor authorized the prohibited activity.

b. Any DUSM who, with supervisory approval, participates in prohibited activity, will within 24 hours of engaging in a prohibited activity, complete a second Form USM-11, that includes a description of the actual prohibited activity in which the DUSM participated, the date(s) and time(s) such activity was engaged in, and the addresses of any prohibited web site accessed by the DUSM.

c. In situations where fast moving investigations may not allow time to complete Form USM-11, describing the prior authorization to engage in the prohibited activity before engaging in the prohibited activity itself, in every such instance, the DUSM participating in such prohibited activity must, within 24 hours of engaging in the prohibited activity, complete Form USM-11 with the information described in E.2.a of this policy directive.

d. Completed Form USM-11, must be immediately provided to the supervisor and CDUSM for review.

3. **Monitoring of Computer and Telecommunications Systems**: Requests to access an employee's computer or telecommunications system for any reason except those specified in section D.3 of this policy directive, such as for suspected misconduct not connected with an official investigation, are to be submitted in writing to the Director or Deputy Director of the USMS. The Deputy Director or CIO shall direct appropriate IT staff to take the actions necessary to execute the authorization.

4. **Reporting of Potential or Actual IT Security Breaches:** Users must immediately notify their superiors and ITD Helpdesk or ITD Security of any suspected breach of security. Notification should be conveyed by e-mail, or telephonically if e-mail is not available. In the event that an initial report is made telephonically, a follow up e-mail should be sent to document the initial report.

5. **Accountable Property Procedures:** See specific procedures related to the management of IT accountable property.

a. Accountable property purchased by ITD and delivered through the headquarters warehouse will be marked as accountable property and entered into the current records systems through the appropriate warehouse procedures.

b. If the property is originally placed on the ITD account, but is later then moved to another office's account, all appropriate forms will be completed to document the transfer of the property from ITD to the receiving office.

c. Accountable property purchased by ITD and delivered through a district or remote division location will be marked as accountable property and entered into the current property records system through the appropriate procedures for the receiving location.

6. **IT Configuration Requests:** Requests to modify IT configurations to current or new IT resources, as well as requests to utilize IT software should be submitted to the Deputy Assistant Director for ITD or delegated ITD official. For standard IT workstation configurations, new hardware and software will be tested by ITD staff prior to installation and use, consistent with the procedures associated with the *Request for Change (RFC)*

process, Appendix 12-7.3. Non-standard IT workstation configurations will also be documented through the RFC.

7. **Funding of IT Hardware, Software, and Telecommunications Equipment and Services:** When a requirement for the purchase of IT hardware, software, or services is identified, the funding source will be determined.

   a. If the purchase is to be part of the CERP program, CERP funds will be used from the ITD work plan.

   b. If the purchase is to be for a special office or function that has separate funds, those funds will be transferred to the ITD division for the purchase.

   c. If the purchase is not part of the CERP program, nor a specially designated purchase, the funding must be identified either from within the ITD work plan or from other agency funding.

8. **Request for the Purchase:** The acquisition of the hardware, software, or services will be made following all applicable regulations, including Policy Directive 6.1, *Procurement Authority and Oversight*, and Policy Directive 6.2, *Acquisition Planning*.

   a. **Detailed Procedures:** The specific procedures to be followed for the IT purchase will depend on the exact items being purchased. ITD is responsible for administering ancillary IT procurement standards and procedures: Appendix 12.2A, *USMS IT System Purchase Standards.*

   b. **Receipt of Items:** It is the responsibility of the obligating office to accurately control, record and report all obligations, including knowing when the items have been received and payment can be made. To the extent that a purchase of an IT resource may be made by ITD but received by another division or a district, communication between the receiving office and ITD must be clear and timely to meet the government's responsibilities for prompt payment of legitimate debts.

9. **Request for Exemptions of Variance from IT Workstation or Printer Allocations:** Requests to acquire IT resources that do not conform to the IT workstation or printer allocations that are specified in this policy will be submitted to the Deputy Assistant Director for ITD or delegated ITD official for review and written approval.

**F. Definitions:**

1. **BlackBerry:** BlackBerry is a line of mobile e-mail devices and services from Research In Motion (RIM). BlackBerry is a complete package that includes airtime, software, and choice of BlackBerry mobile device.

2. **Device:** Any machine or component that attaches to a computer. Examples of devices include disk drives, printers, mice, and modems. These particular devices fall into the category of peripheral devices because they are separate from the main computer. Most devices, whether peripheral or not, require a program called a device driver that acts as a translator, converting general commands from an application into specific commands that the device understands.

3. **E-mail disclaimers** are statements that are either part of a signature block, placed at the end of an e-mail, or appended to e-mails. These statements usually pertain to issues of liability; confidentiality requirements; law enforcement requirements; the nature, security level or type of information contained in the email; contractual specifications;

statements about virus control; and / or other disclaimers associated with the mission of the organization or individual employee. A specific example of a USMS disclaimer is the "Limited Use / Law Enforcement Sensitive" Disclaimer:

> "This information is the property of the U.S. Marshals Service and may be distributed to persons in your agency who have a need-to-know of the sensitive information contained in this email in order to perform an identifiable and authorized government function. Further distribution without the U.S. Marshals' authorization is prohibited. If printed this information must be stored in an approved locked cabinet when unattended and must be destroyed by an approved shredder."

Another example is:

> "Confidentiality Notice: This e-mail, including all attachments, is for the sole use of the intended recipient(s) and may contain law enforcement sensitive, confidential or privileged information. E-mails are protected under the Electronic Communications Privacy Act, 18 U.S.C. 119 Sections 2510, 2511 and 2521. Any unauthorized review, use, disclosure or distribution is prohibited."

4. **E-mail Stationery**: E-mail stationery refers to the use of background templates or images for sending individual e-mail. Depending on the type of email system that is utilized, the user has the ability to create or choose background colors, images or templates for customizing the appearance of their e-mail messages.

5. **Hardware:** Refers to information technology objects such as monitors, central processing units, external devices, disks, disk drives, display screens, keyboards, printers, boards, and chips.

6. **IT Resources:** A term to denote a wide range of hardware, software, and services that comprise information technology that is required to support the USMS mission requirements.

7. **Official correspondence** refers to various types of written communication, i.e., telegrams, memoranda, letters, and electronic messages that are written to convey information to other individuals in the context of performing USMS duties and responsibilities. Official correspondence includes the use of official USMS letterhead, the use of an usms.doj.gov or usdoj.gov email address, or other USMS information management systems to send or convey information to other individuals.

8. **PDA:** An abbreviation for personal digital assistant, a hand-held device that combines computing, telephone/fax, Internet and networking features. A typical PDA can function as a cellular phone, fax sender, Web browser and personal organizer.

9. **Plain Text:** Plain text refers to the absence of custom fonts, images, symbols, and other style formats that are commonly available in e-mail, word processing, and web content programs.

10. **Portable:** When used to describe hardware, portable means small and lightweight. A portable computer is a computer small enough to carry. Portable computers include notebook and subnotebook computers, hand-held computers, palmtops, and PDAs. When used to describe software, portable means that the software has the ability to run on a variety of computers. Portable and machine independent mean the same thing—that the software does not depend on a particular type of hardware.

11. **Printer:** A device that prints text or illustrations on paper. There are many different types of printers based on the technology utilized, the range of functions provided in a given device, the quality of type, speed of printing, impact or non-impact type, graphics, and fonts.

12. **Rich Text Format** (RTF) is a proprietary document file format developed by Microsoft Corporation. It is a specific type of **formatted text**, styled text or rich text, as opposed to plain text, and has styling information beyond the minimum of semantic elements: colors, styles (boldface, italic), sizes and special features.

13. **Signature Block:** A signature block or e-mail signature (often abbreviated as signature, sig block, sig file, .sig, dot sig, or sig) is a block of text automatically appended at the bottom of an e-mail message. This has the effect of "signing off" the message and in a reply message of indicating that no more response follows. It is common practice for a signature block to consist of one or more lines containing some brief information on the author of the message.

13. **Software:** Computer instructions or data. Anything that can be stored electronically is software. The storage devices and display devices are hardware. Software is often divided into two categories: systems software, which includes the operating system and all the utilities that enable the computer to function; and applications software, which includes programs where the user has direct involvement with processing work. For example, word processors, spreadsheets, and database management systems fall under the category of applications software.

14. **Trusted Internet Connection Initiative:** (also known as TIC), is mandated by the Office of Management and Budget (OMB) Memorandum M-08-05, issued in November 2007. The memorandum specifies a policy that intends to optimize individual external connections for Federal Government agencies, including Internet points of presence currently in use by the Federal Government of the United States. It includes a program for improving the Federal Government's incident response capability through a centralized gateway monitoring at a select group of TIC Access Providers (TICAP). (Reference: OMB memorandum M-08-16, *Guidance for Trusted Internet Connection Statement of Capability Form.*)

15. **Wi-Fi:** Technology that uses radio waves to provide wireless high-speed Internet and network connections. The Wi-Fi Alliance, the organization that owns the Wi-Fi (registered trademark) term specifically defines Wi-Fi as "any wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards."

**G. Cancellation:** Supersedes USMS Policy Directive 12.2, *The Management, Use, Allocation, Deployment, and Accountability of United States Marshals Service (USMS) Information Technology (IT) Resources and Systems*.

**H. Authorization Date and Approval:**

**By Order of:** **Effective Date:**

/S/ 2/2/11

Stacia A. Hylton
Director
U.S. Marshals Service

## 12.3 Information Technology Account Management and User Support

**A. Proponent:** Chief Information Officer (CIO), Assistant Director (AD), Information Technology Division (ITD). Telephone: 703-604-2054, Fax: 202-307-5130.

**B. Purpose:** To establish United States Marshals Service (USMS) policy governing the creation and use of Information Technology (IT) and Information Resources (IR), user accounts, and user support for USMS staff. This policy applies to all persons who use USMS IT resources, including but not limited to employees, contractors, Task Force Officers (TFOs), and interns. This policy applies to classified and unclassified computer and telecommunications systems, technology, peripheral devices, and resources that are acquired for use by, owned, operated, or managed by USMS offices and users.

**C. Authority:** References to selected laws and regulations applicable to this policy directive are listed in Policy Directive 12.1, *Information Resources Technology Management*, Appendix 1, *Authority*.

**D. Policy:**

1. Access to IT and IR systems: Only personnel who have undergone a background investigation which has been favorably adjudicated by the USMS, have been accepted under reciprocity by the USMS, and/or granted extra-Department of Justice (DOJ) access (e.g., through a Memorandum of Understanding (MOU) or via Regional Information Sharing Systems Network (RISSNET) or Law Enforcement Online (LEO)) may be provided access to and use of USMS computer and telecommunication systems.

2. Initiation, moves, and termination of IT user accounts and IT systems access:

   a. District/division approving authorities are responsible for requesting access to and use of USMS workstations, IT systems, and telecommunications systems for users requiring access; and

   b. District/division approving authorities are responsible for requesting the closure of IT systems accounts or access to IT systems for staff that have separated from the USMS, and/or no longer require access to a particular IT system.

**E. Responsibilities:**

1. The AD, ITD, who also serves as the CIO, is responsible for:

   a. Recommending USMS-wide policies, standards, procedures, and guidelines for USMS IT systems user access, support, and IT system account management; and

   b. Delegating user support and account management responsibilities as necessary for the effective and efficient operation of the USMS IR classified and unclassified program and IT systems.

2. The AD, Tactical Operations Division (TOD), is responsible for:

   a. Reviewing and processing requests for background investigations and favorable adjudications for USMS staff, TFOs, contractors, and individuals detailed to the USMS. The type of background investigation is dependent upon the position designation level. A completed background investigation is mandatory for access to IT and IR systems for USMS staff and contractors; and

   b. Recommending USMS-wide policies, standards, procedures, and guidelines for USMS secure telecommunications, IT systems, and account management.

3. ITD is responsible for providing IT and IR support to USMS staff.

4. TOD is responsible for the management and provision of support services for secure telecommunications equipment and reviewing and processing background investigations and favorable adjudications.

**F. Procedures:**

1. All requests for exceptions to this policy are to be submitted in writing (e-mail is acceptable) to the CIO, who directs the request to the appropriate USMS official for approval.

2. Procedures associated with the management, use, allocation, deployment, and accountability of USMS IT resources and systems are found in Policy Directive 12.2, *The Management, Use, Allocation, Deployment, and Accountability of United States Marshals Service Information Technology (IT) and Resources and Systems*.

3. Access to USMS IT and IR systems:

   a. Requests for background investigation and favorable adjudication are processed through the Office of Security Programs, TOD.

   b. IT Systems Access Requests:

      1) New USMS employees and contractors requiring an IT user account must complete Form USM-169, *User Account Request* (UAR). Form USM-169 is signed and submitted via e-mail by the employee's/contractor's approving authority to the ITD Help Desk at ITS.Helpdesk@usdoj.gov. Certain IT systems may require additional forms which are specified on Form USM-169;

      2) New users must also complete the USMS Rules of Behavior (ROB). The approving authority electronically submits the ROB form with Form USM-169 to the ITD Help Desk. Refer to Standard Operating Procedures: Account Management v1.12 Section 6.1, *In-Processing*;

      3) When an employee and/or contractor leaves the USMS and/or no longer requires access to IT systems, Form USM-169 is e-mailed to the ITD Help Desk by the appropriate Administrative Officer (AO) prior to the employee's or contractor's departure;

      4) The DOJ ROB for Privileged Users is signed by all users designated as having elevated privileges to USMS computer resources, and is required in addition to the Computer System User IT Security General ROB to

which all users are subject. Electronic copies of the signed ROBs are forwarded to the ITD Help Desk;

5) Signed ROBs are retained by districts/divisions for recordkeeping and audit purposes. Electronic copies of the signed ROBs are forwarded to the ITD Help Desk; and

6) The ITD Help Desk assigns account requests to ensure proper coordination with affected ITD components.

4. IT support procedures:

a. Procedures for creation, modification, deletion, and/or disablement of USMS user accounts and IT systems access are found in Standard Operating Procedures: Account Management v1.12; and

b. ITD General Report Procedures are incorporated in this policy by reference.

**G. Definitions:**

1. **Account:** A logical representation of a user in a system, which allows a user to gain access to the system. Examples of user accounts are: Microsoft Active Directory Service accounts, UNIX accounts on individual servers, Oracle database accounts, application accounts (JDIS, FMS, and M-WISE), and accounts on devices such as Local Area Network (LAN) infrastructure equipment.

2. **Account Deletion:** The process that permanently removes an account.

3. **Account Disablement:** The process that disables an account. Disabling does not delete an account; it prevents access to a USMS system or application.

4. **Account Management:** The processes that govern account creation, modification, disablement, monitoring, and reporting.

5. **Account Modification:** The process of changing details related to an account, including location and level of access.

6. **Approving Authority:** An authorized person approving all account management access requests for an office, district, division, and/ or task force office. Generally, that person is a designated signatory identified by the office or division and has received training in account management. For purposes of this document, references to the approving authority correspond to the following division, district office, and/or task force positions: Director, Deputy Director, Associate Director, AD, Deputy Assistant Director, Branch/Office Chief, United States Marshal, Chief Deputy United States Marshal, Assistant Chief, Operations or Administrative Supervisor, and/or AO.

7. **Privileged User:** A privileged user is someone who authorizes access to DOJ, USMS, or other government computer resources when that access provides the capability to alter the properties, behavior, or control of DOJ information system(s) and/or network(s). Privileged use includes, but is not limited to, any of the following types of access:

a. “Super user,” “root,” or equivalent access, such as access to the control functions of the information system(s)/network(s) or administration of user accounts;

b. Access to change control parameters (e.g., routing tables, path priorities, addresses) of routers, multiplexers, and other key information system(s)/network(s) equipment or software;

c. The ability and authority to control and change program files and other users' access to data;

d. Direct access to operating system level functions (also called unmediated access) that permits system controls to be bypassed or changed; and

e. Access and authority for installing, configuring, monitoring, and/or troubleshooting the security monitoring functions of information systems/networks (e.g., network/system analyzers and intrusion detection software).

8. **RISSNET:** National network comprised of six multistate centers designed to operate on a regional basis to support law enforcement efforts nationwide to combat illegal drug trafficking, identity theft, human trafficking, violent crime, terrorist activity, and also to promote officer safety.

9. **LEO:** 7 days a week, 24 hours a day online (real-time), controlled-access communication and information sharing data repository. It provides an Internet accessible focal point for electronic Sensitive But Unclassified (SBU) communication and information sharing for international, federal, state, local, and tribal law enforcement agencies. LEO also supports antiterrorism, intelligence, law enforcement, criminal justice, and public safety communities worldwide. Users anywhere in the world can communicate securely using LEO.

10. Other definitions can be found in Policy Directive 12.1, *Information Resources and Technology Management*, Appendix 2, *Definitions*.

**H. References:** None.

**I. Cancellation Clause:** This policy directive supersedes Policy Directive 12.3, *User Access to USMS IT User System.*

**J. Authorization and Approval Date:**

| **By Order of:** | **Effective Date:** |
|---|---|
| /S/ | August 30, 2012 |
| Stacia A. Hylton,<br>Director<br>U.S. Marshals Service | |

## 12.4 Telecommunications

**A.** **Proponent:** Assistant Director for Information Technology Division (ITD)/Chief Information Officer (CIO), Deputy Assistant Director for Information Technology, Chief of Operations and Infrastructure, 202-307-9325. For secure telephone and facsimile equipment and services: Assistant Director for Tactical Operations Division (TOD), 202-353-0389.

**B.** **Purpose:** To provide policy and guidance to all elements in the United States Marshals Service (USMS) for the acquisition, management, and use of network and telecommunications services and equipment.

**C.** **Authority:** Department of Justice (DOJ) Order 2880.1B, Information Resource Management Program; DOJ Order 2640.2F, Information Technology Security; DOJ Order 2420.2, Telecommunications Policy and Guidelines; DOJ Order 2740.1A, Use and Monitoring of DOJ Computers and Computer Systems; DOJ 2421.1E, Use of Government Telecommunications Systems; USMS Policy Directive 1.1, Delegation of Authority, Organization and Functions; Office of Management and Budget (OMB) Memorandum M-08-05.

**D.** **Policy:**

1. **Telephone Service:** All telephone services are acquired from General Services Administration (GSA) if available and cost-effective.

2. **Use of the Federal Telecommunications Systems (FTS 2001):** FTS 2001 is the mandated, inter-city long distance telecommunications system for use by the USMS. FTS 2001 is used to the maximum extent possible for placing official long distance calls to conduct business. Employees are authorized use of FTS 2001 for other than official business as stated in DOJ Order 2421.1E.

   a. An employee injured on the job may place calls as necessary to notify his / her family and doctor.

   b. An employee traveling on government business with a need to reschedule a return time due to official business or transportation delay may place a call to notify his / her family of the change in schedule.

   c. An employee traveling more than one night on government business may make a brief call (not to exceed five minutes) daily to his / her residence.

   d. An employee required to work overtime without advance notice may place a call to notify his / her family of the change in schedule, or to make alternate transportation or childcare arrangements.

   e. An employee may make a brief call daily to locations within the local commuting area (the area from which the employee regularly commutes) to speak to spouse, minor children, or those responsible for them (e.g., school or day-care center).

f. An employee may make a brief call daily to locations within the local commuting area that can only be reached during working hours, such as his / her residence, a local government agency, or a physician's office.

g. An employee may make a brief call to locations within the local commuting area to arrange for emergency repairs to his / her residence or automobile.

3. **Long-Distance (LD) Telephone Service:** FTS 2001 is used exclusively for all calls, with the exception of international calls. All LD calls must be limited to official business, or those authorized by DOJ Order 2421.1E.

4. **Local Company Provided Telephone Service:** If FTS 2001 telephone services are not available from GSA, commercial service must be obtained from the local telephone company.

5. **Wireless Voice and Data Cellular Telephones and Service:** ITD is responsible for the administration of all wireless devices and systems, both on and off the USMS network.

6. **Acquisition of Wireless Goods and Services Cellular Telephones:** This acquisition is made through the wireless strategic sourcing initiative which is comprised of Blanket Purchase Agreements (BPAs) for wireless goods and services.

7. **Allocation of USMS Issued Wireless Devices or BlackBerrys:** Absent specific authority and approval granted by the Wireless Services Board, an employee is issued a single device to facilitate voice and data wireless services (i.e., an employee may not carry a BlackBerry for data service and a voice-only handset for voice service, one BlackBerry per designated employee). The approving authority in a division or district determines who requires a BlackBerry device based on mission requirements and the responsibilities of the position. This is not applicable to the issuance of a data connection / aircard.

   a. Unless documented in writing by exception, the following positions receive one BlackBerry device: Director, Deputy Director, Associate Directors, Assistant Directors, Deputy Assistant Directors, Branch Chiefs, Chiefs, Assistant Chiefs, Supervisors, United States Marshals, Chief Deputy United States Marshals, Assistant Chief Deputy United States Marshals, Supervisory Deputy United States Marshals, Deputy United States Marshals, Criminal Investigators, and Administrative Officers.

   b. Approving authorities in division and district offices have the discretion to allocate wireless devices / BlackBerrys to division staff (e.g. analysts, specialists, and investigator levels) and district administrative staff.

   c. Approving authorities have the discretion to allocate wireless devices / BlackBerrys to contract staff based on the mission requirements and responsibilities associated with the position. The requirement must be documented in writing and submitted to the CIO.

   d. USMS issued wireless devices / BlackBerrys are not issued to Task Force officers from other law enforcement agencies, guard functions, court security officers, or intern positions.

   e. Requests for exceptions to the allocation guidelines set forth in this policy require CIO approval, and are made via e-mail.

8. **Modification of Wireless Goods and Services Cellular Telephones:** USMS employees are not authorized to make changes to the goods, devices, or services available through the wireless BPAs and, absent specific authority and approval granted by the Wireless Services Board, employees are not authorized to expend government funds to purchase wireless devices, goods, and services outside the BPAs. Changes must be approved by the Contracting Officer for the BPAs.

9. **Wireless Voice and/or Data Cellular Telephone Service:** Due to high installation costs and recurring utilization charges, this service is procured only when there is a specific mission requirement and such service is deemed cost-effective.

10. **Wireless Voice and/or Data Mobile Device/Cellular Telephone Access Protection:** USMS employees are responsible for securing and protecting access to USMS issued wireless devices.

    a. Where technically feasible (supported by the wireless cellular unit), access to a wireless cellular device's telephone call records and address book should be protected by a password or personal identification number (PIN). This is to ensure lost or stolen wireless devices and cellular telephone information is not disclosed to outside parties. Information stored on USMS official BlackBerry devices is automatically encrypted through the security policy settings.

        1) Data security is achieved with a BlackBerry and a device is unlocked in eight to ten seconds using the unique eight-character password.

    b. Government data must not be maintained within personal wireless devices.

11. **Oversight and Use of Wireless Services and Devices:** ITD is responsible for monitoring monthly wireless data utilization patterns associated with BlackBerry devices and/or data connection/aircards. A BlackBerry end user, whose device demonstrates inactivity for thirty days or more, is subject to having his / her BlackBerry user account removed from the BlackBerry Enterprise Servers (BES). An employee who is no longer employed by the USMS must have his / her user account removed from BES immediately.

    a. As a cost-savings measure, districts and divisions must consider temporarily suspending or disconnecting wireless voice and/or data service for an end user who is without remote access to USMS systems for an extended period of time (e.g., extended leave, or missions in foreign countries that do not support voice and/or data networking service). In an effort to preserve the telephone number with a specific account, some service providers offer plans to suspend voice service for a nominal fee that is usually less costly than the standard monthly access fee. Districts and divisions are authorized to consider this option when suspending or disconnecting service for users for a specified period of time.

    b. Wireless services are provided to support mission-related requirements with limited authority for personal use where there is no direct cost to the USMS.

    c. Wireless program managers and ordering officers are responsible for monitoring usage patterns of wireless devices and conducting trend analyses through reports generated and supplied by vendors. Instances of apparent misuse of wireless devices such as excessive text messaging, high peak voice minutes unrelated to USMS business, ring-tone, game, and/or music downloads, and other non-mission-related activity may be reported to an employee's supervisor and other USMS officials in conformance with USMS reporting practices associated with the misuse of government property and services.

d. Wireless Voice and/or Data Usage: A USMS-issued wireless device is subject to monitoring and employees have no expectation of privacy in usage.

e. Employees may be disciplined for misuse of wireless privileges, and may be held financially responsible for such misuse that results in a cost to the district or division.

f. Directory Assistance: Fee-for-service directory assistance (411 or 555-1212) must not be utilized in lieu of the more preferred toll-free directory assistance service such as GOOGLE 411 (800-GOOG411 or 800-466-4411). Other similar toll-free services are available from select providers.

g. To avoid costly international toll charges to wireless accounts, telephone calls using a wireless device for international destinations are patched through the USMS Communications Center by calling 800-336-0102 and providing the operator the desired international telephone number. The operator dials the international destination on behalf of the user.

12. **Lost, Misplaced, or Stolen Wireless Cellular Telephones or BlackBerry Devices:** If a wireless device, cellular telephone, or BlackBerry is lost, misplaced or stolen, the assigned user of the device is responsible for immediately notifying the office that issued the device to request the deactivation of voice service. For BlackBerry devices, the user should also immediately notify the ITD Help Desk, 202-307-5200. ITD technicians will disable data services to the device and remotely erase information contained on the device.

13. A BlackBerry device is considered accountable property and control and safeguarding is treated in accordance with Policy Directive 7.1, *Management of Personal Property*.

14. **Telephone Credit Cards:** Telephone credit cards will be issued on an exception basis. USMS District or Headquarters Division offices should conduct an internal assessment of their respective organizations to determine if the calling cards still represent a valid operational requirement. The assessment should consider the utility of using handheld devices (Blackberry and Cellular Phones) that are currently utilized to fulfill the requirements typically provided by telephone credit cards. Replacement cards will not be issued automatically. If an office determines that the calling card is required to successfully accomplish mission requirements, an e-mail request should be submitted to ITD. The request should specify name, district/division office, office address, telephone number, if international access is required, and a general explanation for the need for the calling card.

15. **Telephone Cards for Overseas Calls:** For those USMS personnel who, in the performance of their duty, require the ability to call overseas using a telephone credit card, standard commercial telephone cards must be obtained.

16. **Return/Reissue of Credit Cards:** USMS credit card holders, upon reassignment within the Service, must take their credit card with them to their new assignment.

a. It is the responsibility of the program manager or supervisor of the losing district/division to notify ITD when a transfer occurs so that the inventory database can be updated. The information provided must include the employee's name, credit card or sequence number, the office he/she is leaving, and the new office that he/she is assigned to.

b. When personnel retire or transfer out of the USMS, the same notification must be made and the credit card must be retrieved and returned to ITD.

17. **Use of Telephone Credit Cards:** FTS telephone credit cards and commercial telephone credit cards are for ''Official Use Only'' with the following exception: during official travel away from the normal duty station, USMS personnel are authorized to place one call a day to their home. This call will be limited to five minutes and must be charged against the FTS telephone credit card.

18. **Unsolicited Credit Cards:** Unsolicited credit cards must be returned to the sender with a letter containing the following statement:

''The unsolicited telephone credit cards with the following control numbers have been received by (organizational name) and are hereby returned. (List numbers and addresses shown on each card). The purpose of this letter is to inform you that the (organizational name above) will neither honor nor pay any charges placed against the above cards. Additionally, we will neither honor nor pay charges placed against any credit card issued to the USMS or its components which was not specifically requested and received by an authorized official of this organization.''

19. **Lost or Stolen Credit Card:** Should a credit card become lost or stolen, the card holder must notify his/her issuing office immediately and follow up with confirming correspondence to ITD for appropriate action.

20. **Telephone Maintenance Agreements:** After the expiration of the one year warranty on a district's new telephone system, a telephone maintenance agreement is entered into by each district office with the vendor who provided and installed the telephone systems located in the district or sub-offices.

a. The cost for the initial maintenance agreement is reimbursed by ITD for the remainder of the current fiscal year. Districts must budget for future maintenance agreements in their yearly workplan.

b. This agreement is for all multi-button instruments and accessories. No single line instruments are placed on the agreement, as replacement of these sets is more cost-effective due to their relatively low cost.

21. **Facsimile (Fax) Transceivers:** Basic fax units are provided to all staffed USMS offices.

a. Fax units are procured locally from a vendor that can provide the equipment that meets the particular needs of the office.

b. Fax machines that have network capabilities cannot be connected to the USMS network without written approval from ITD.

c. District offices are responsible for issuing renewal Purchase Orders for all leased fax machines under their purview, effective October 1 of each fiscal year. These renewal Purchase Orders are submitted directly to the authorized vendor.

d. Headquarters organizations must submit a Form USM-157, *Requisition for Procurement of Supplies, Service, and Equipment,* for yearly renewals to the Chief, Contract Administration Branch, Procurement Office.

e. Facsimile Telephone Line Acquisition: Requests for telephone lines to support fax machines are submitted to ITD. Requests must include the location of the machine, the telephone number, and name of the point-of-contact. ITD

processes the request through appropriate channels and reimburses the district/division for all costs associated with the installation after receiving copies of the paid invoice(s) and a request for reimbursement.

22. **USMS Network:** The USMS network infrastructure (MNET) is provided as a central utility for all users of USMS Information Resources (IR). Any activities related to the network (e.g., connecting computer or telecommunications equipment) must be performed or specifically directed by ITD personnel.

    a. Users are permitted to use only those network addresses issued to them by ITD.

    b. All remote access (dial in services, dial out services, virtual private network (VPN)) to MNET is through an approved remote access system (RAS).

    c. Devices used on MNET (e.g., handhelds, personal computers (PCs), laptops) must not be connected to MNET at the same time a modem or other external access point (i.e., alternate network connection) is connected to the device. This includes users utilizing a RAS.

    d. Users must not extend or re-transmit network services in any way. No router, switch, hub, dual network card, modem, or wireless access point to the USMS network is installed without prior approval.

    e. Users must not install network hardware or software that provides network services.

    f. Non-USMS computer systems (e.g., state/local law enforcement systems, personally owned systems) must not be connected to MNET.

    g. Users must not download, install, or run security programs or utilities that reveal weaknesses in the security of a system. For example, USMS users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the MNET network infrastructure, nor are USMS users permitted to run such programs against USMS information even while not connected to the USMS network (e.g., downloading a USMS password or database file and then running a cracker program against it on a home computer is not allowed).

    h. Users are not permitted to alter network hardware in any fashion.

    i. Users are not permitted to use USMS-provided computer or telecommunications systems to connect to external networks without written approval.

    j. No infrared or wireless networking technologies shall be implemented to transmit USMS data without written approval.

## E. Procedures:

1. **Obtaining GSA Provided Telephone Services:** District or Division offices should send an e-mail request to the ITD Help Desk ( its.helpdesk@usdoj.gov ). The request will be assigned to the ITD Infrastructure Office, Telecommunications Section. The Telecommunications Section will coordinate the request with the appropriate district or division office and the GSA regional office.

2. **Requests for FTS 2001 Service:** Requests must contain the street address or location where the service is desired; along with name, address and telephone number of

person(s) to be contacted for additional information and installation coordination. Requests for this service are submitted in writing to ITD for review, approval, and submission to the GSA regional office for implementation.

3. **Local Company Provided Telephone Service:** Any services procured through the local telephone company must be approved in advance by ITD. District or Division offices should send an e-mail request to the ITD Help Desk ( its.helpdesk@usdoj.gov ). The request will be assigned to the ITD Infrastructure Office, Telecommunications Section. The Telecommunications Section will coordinate the request with the appropriate district or division office. Once the commercial service is installed, ITD must be notified so an order can be placed for Switched-On-Net FTS 2001 service through the government carrier, United States Sprint. ITD reimburses a district work plan for the costs incurred for installation of the commercial service, upon receipt of a paid invoice with voucher stamp.

4. **Acquisition of Wireless Goods and Services Cellular Telephones:** Purchases will follow the normal USMS procurement process through the use of the wireless strategic sourcing initiative BPAs. Comprehensive information on the program is maintained on the USMS Intranet at the Wireless web page at http://156.9.232.31/it/wireless/index.html.

5. Requests to approve alternate wireless devices or services through the BPAs may be submitted to the Wireless Services Board via e-mail to wireless.usms@usdoj.gov. In order for a device or service to be included in the BPAs, an extensive technical and price/performance evaluation will be completed, the Board will review, and modifications to the BPAs may be issued by the Contracting Officer, as required. The Board will only consider changes that provide a substantial benefit to USMS missions, over and above current offerings, and at a cost benefit to the USMS. Wireless Services Board decisions may be appealed to the CIO, whose decision will be final.

6. Remote e-mail service is provided to end users through the USMS BES. Access to the BES, or troubleshooting with wireless devices, may be obtained by contacting the USMS ITD Help Desk at 202-307-5200.

7. **Issuing Telephone Credit Cards:** Each USMS organization requiring FTS telephone credit cards will submit a written request (e-mail is acceptable) to ITD with the following information:

   a. Individual's name;

   b. Individual's social security number; and

   c. Individual's duty office.

   ITD will then issue an FTS telephone credit card to the individual with an inventory sheet that must be signed and returned. A master list identifying the card number, holder, issuing date, and justification will be maintained by ITD.

8. **Telephone Cards for Overseas Calls:** For those USMS personnel who, in the performance of their duty, require the ability to call overseas using a telephone credit card (standard commercial telephone card) must obtain prior permission.

   a. For Headquarters, district, and field office personnel, a written request (e-mail is acceptable) will be submitted to ITD with the following information:

      1) Individual's name;

2) Individual's social security number; and

3) Individual's duty office.

b. For district personnel, an indication as to whether, in the performance of their duty, the ability to call overseas using a telephone credit card is required.

9. **Establishing District Telephone Maintenance Agreements:** Each district office should contact their local vendor and request a maintenance proposal for all of the instruments placed on the agreement.

a. Copies of the proposals are forwarded to ITD along with a written request to purchase this agreement on a local purchase order.

b. Once approved, ITD advises the district to initiate the maintenance agreement.

c. Reimbursement is accomplished in accordance with reimbursement procedures for the remaining months of that fiscal year.

d. Maintenance covers the telephone instruments, instrument features and auxiliary devices, cabling, common equipment components, and all wiring between the instrument and the point of entry of the telephone company dial tone wiring.

e. Annual charges for such maintenance are per instrument on a flat rate basis.

10. USMS offices that have Secure Terminal Units, third generation (STU-III) telephones must contact the USMS Communications Security (COMSEC) Manager, OSP, TOD, and request secure telephone equipment replacement and disposition instructions.

**F. Definitions:** Refer to 12.4, Appendix 1 for definitions.

**G. Cancellation Clause**: Supersedes Policy Directive 12.4, *Telecommunications*.

**H. Authorization and Date of Approval:**

| **By Order of:** | **Effective Date:** |
|---|---|
| /S/ | 8/23/10 |
| John F. Clark<br>Director<br>U.S. Marshals Service | |

## 12.4 Telecommunications: Appendix 1

**Definitions:**

1. **Facsimile machine:** In telecommunications, the transmission and reproduction of documents by wire or radio wave. Common fax machines are designed to scan printed textual and graphic material and then transmit the information through the telephone network to similar machines, where facsimiles are reproduced close to the form of the original documents.

2. **Facsimile transceiver:** In a facsimile system, the equipment that sends and receives facsimile signals. (188) Note: Full-duplex facsimile transceivers can send and receive at the same time; half-duplex facsimile transceivers cannot.

3. **FTS 2000 and FTS 2001:** Federal Telecommunications System 2000 (FTS2000) is a long distance telecommunications service for the United States federal government, including services such as switched voice service for voice or data up to 4.8 kbit/s, switched data at 56 kbit/s and 64 kbit/s, switched digital integrated service for voice, data, image, and video up to 1.544 Mbit/s, packet switched service for data in packet form, video transmission for both compressed and wideband video, and dedicated point-to-point private line for voice and data. The use of FTS2000 contract services is mandatory for use by U.S. Government agencies for all acquisitions subject to 40 U.S.C. 759. No U.S. Government information processing equipment or customer premises equipment other than that which are required to provide an FTS2000 service are furnished. FTS2000 contractors are required to provide service directly to an agency's terminal equipment interface. GSA awarded two 10-year, fixed-price contracts covering FTS2000 services on December 7, 1988. The Warner Amendment excludes the mandatory use of FTS2000 in instances related to maximum security. FTS2000 was completed in 2000, and was replaced by FTS2001. Federal and other government-owned long distance telephone systems provide a cost effective means to satisfy Government requirements for long distance inter-city communications. The FTS 2001 operates on a station-to-station basis among government offices throughout the continental United States, Alaska, Hawaii, Guam, Puerto Rico, and the Virgin Islands.

4. **Internet telephony**: Internet telephony refers to communications services—voice, facsimile, and/or voice-messaging applications—that are transported via the Internet, rather than the public switched telephone network (PSTN). The basic steps involved in originating an Internet telephone call are conversion of the analog voice signal to digital format and compression/translation of the signal into Internet protocol (IP) packets for transmission over the Internet; the process is reversed at the receiving end.

5. **Integrated Services Digital Network (ISDN):** ISDN is a telephone system network. The key feature of the ISDN is that it integrates speech and data on the same lines, adding features that were not available in the classic telephone system. There are several kinds of access interfaces to the ISDN defined: Basic Rate Interface (BRI), Primary Rate Interface (PRI) and Broadband-ISDN (B-ISDN). ISDN is a circuit-switched telephone network system hat also provides access to packet switched networks, designed to allow digital transmission of voice and data over ordinary telephone copper wires, resulting in better voice quality than an analog phone. It offers circuit-switched connections (for either voice or data), and packet-switched connections (for data).

6. **KOV-14 Fortezza Plus PC card** provides encryption functions and key storage to the Secure Terminal Equipment (and other devices). It is a tamper-resistant module based on the Mykotronx Krypton chip, including all of the cryptographic functionality of the original Fortezza card plus the Type 1 algorithms/protocols BATON and FIREFLY, the SDNS signature algorithm, and the STU-III protocol. It was developed by Mykotronx as

part of the NSA's MISSI program. As of 2008, the KOV-14 is beginning to be phased out and replaced by the KSV-21 PC card.

7. **KSV-21** is a PC card built by Mykotronx as a tamper-resistant reprogrammable module and is backwards compatible with the KOV-14 Fortezza Plus card. It adds features including support for SCIP, Enhanced Firefly and NSA's 21st century Key Management Initiative. It can perform Type 1 encryption operations at 80 Mbit/s. As of 2008, the KOV-14 is beginning to be phased out and replaced by the KSV-21. The U.S version is certified to protect classified data through the Top Secret/SCI level as well as unclassified sensitive information. Versions are available for use with other nations, including: Canadian national (KSV-22); Combined Communications Electronics Board (CCEB) (KSV-30); NATO (KSV-40); Coalition Partners (SSV-50)

8. **Long Distance Telephone Service (LD):** The term ‘‘long distance’’ (LD) generally refers to all calls made outside a local service or calling area.

9. **Secure Data Network System (SDNS):** The Secure Data Network System (SDNS) project, implements computer to computer communications security for distributed applications. The internationally accepted Open Systems Interconnection (OSI) computer networking architecture provides the framework for SDNS. SDNS uses the layering principles of OSI to implement secure data transfers between computer nodes of local area and wide area networks. Four security protocol documents developed by the National Security Agency (NSA) as output from the SDNS project are included. SDN.301 provides the framework for security at layer 3 of the OSI Model. Cryptographic techniques to provide data protection for transport connections or for connectionless-mode transmission are described in SDN.401. Specifications for message security service and protocol are contained in SDN.701. Directory System Specifications for Message Security Protocol are covered in SDN.702.

10. **Secure Terminal Equipment (STE): STE** is the U.S. Government's current, encrypted telephone communications system for wired or "landline" communications. STE is designed to use standard public switched telephone network (PSTN) lines or ISDN telephone lines which offer higher speeds of up to 128k b per second and are all digital. The greater bandwidth allows higher quality voice and can also be utilized for data and fax transmission through a built-in RS-232 port. STE is intended to replace the older STU-III office system and the KY-68 tactical system. STE sets are backwards compatible when using a KOV-14 card with STU-III phones, but not with KY-68 sets. STE sets look like ordinary high-end office desk telephones and can place unsecured calls to anywhere on the public switched telephone network (PSTN). There is a PC Card slot in the STE that allows a Fortezza Plus (KOV-14) Crypto Card or KSV-21 Enhanced Crypto Card to be inserted. When an NSA configured Crypto Card is present, secure calls can be placed to other STE phones. STE phones are upgradable (unlike STU-III sets). All cryptographic algorithms are in the crypto card. Newer STE sets can communicate with systems that use the Secure Communications Interoperability Protocol (SCIP) (formerly Future Narrowband Digital Terminal (FNBDT)). There are upgrades available for older units.

11. **Security Token:** A security token (sometimes called an authentication token) is a small hardware device that the owner carries to authorize access to a network service. The device may be in the form of a smart card (e.g. KSV-21) or may be embedded in a commonly used object such as a key fob. Security tokens provide an extra level of assurance through a method known as two-factor authentication: the user has a personal identification number (PIN), which authorizes them as the owner of that particular device; the device then displays a number which uniquely identifies the user to the service, allowing them to log in. The identification number for each user is changed frequently, usually every five minutes or so. Unlike a password, a security token is a physical object.

A key fob, for example, is practical and easy to carry, and thus, easy for the user to protect. Even if the key fob falls into the wrong hands, however, it can't be used to gain access because the PIN (which only the rightful user knows) is also needed.

12. **STU-III:** STU III is a family of secure telephones introduced in 1987 by the NSA for use by the United States government, contractors, and allies. The STU-III is being phased out of service as of December 31, 2009.

13. **Voice over Internet Protocol (VoIP):** A general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks. Other terms frequently encountered and synonymous with VoIP are IP telephony, Internet telephony, voice over broadband (VoBB), broadband telephony, and broadband phone. VoIP systems employ session control protocols to control the set-up and tear-down of calls as well as audio codecs which encode speech allowing transmission over an IP network as digital audio via an audio stream. Codec use is varied between different implementations of VoIP (and often a range of codecs are used); some implementations rely on narrowband and compressed speech, while others support high fidelity stereo codecs.

14. **Wireless Services Board:** This is a designated group of operational and administrative employees to adjudicate the USMS wireless program, including consideration of new devices and services.

15. **Wireless Cellular Telephone Service** refers to a communications network infrastructure that allows individual wireless cellular devices, such as mobile telephones or BlackBerry devices, to interface with the local telephone company. Cellular describes a type of communications system that divides a geographic region into sections, called cells. The purpose of this division is to make the most use out of a limited number of transmission frequencies. Each connection or conversation requires its own dedicated frequency, and the total number of available frequencies in a given area is limited. To support more simultaneous voice or data transmissions, cellular systems allocate a set number of frequencies for each cell.

16. **Wireless Device:** A wireless device refers to a piece of computer equipment or telephone equipment that does not rely on physical wired connections between a sender and receiver but utilizes a communications network that relies on radio waves and or micro waves to maintain communications.

## 12.5 Information Resources Management (IRM)/System Development Life Cycle (SDLC)

**A. Proponent:** Assistant Director for Information Technology Division (ITD) and Chief Information Officer (CIO). Telephone: 703-604-2054, Fax: 202-307-5130.

**B. Purpose:** This policy directive contains Information Technology (IT) IRM/SDLC. The IRM process provides a framework and assigns responsibilities for the United States Marshals Service (USMS) to effectively manage its IT investments in a way that demonstrates good stewardship; complies with applicable laws; and ensures the effective, efficient, and economical accomplishment of USMS's many diverse missions. This policy is applicable to all USMS IT investments, regardless of the dollar amount.

**C. Authority:** References to selected laws and regulations applicable to this policy directive are listed in Policy Directive 12.1, *Information Resources and Technology Management*, Appendix 1, *Authority*.

**D. Policy:** The IRM process:

1. Is to be used to budget for and prioritize the results of deployed IT investments.

2. Provides for a structured, repeatable, and documented process to select, manage, and evaluate IT investments throughout the systems life cycle.

3. Is integrated with the processes for making strategic planning, budget, acquisition, and program management decisions.

4. Is integrated with a structured SDLC methodology which pertains to activities associated with individual investments and includes addressing security issues (e.g., a configuration management process for approving system changes, risk assessments).

5. Requires comparison and prioritization of IT investments based on, at a minimum:

   a. The extent to which the investments contribute to the fulfillment of missions and goals contained in the Department of Justice (DOJ) and USMS Strategic Plans;

   b. The risk associated with the investment;

   c. The return on investment (in terms of both overall affordability for USMS and reasonableness of the individual investment); and

   d. The identification of investments that would result in shared benefits or costs for various USMS districts/divisions, other DOJ components, federal agencies, and/or state/local governments.

6. Enables executives and managers to obtain timely information to monitor the progress of an investment in accordance with established cost, schedule, and performance metrics by identifying, on an independently verifiable basis, when there are significant (i.e., greater than 10 percent) deviations from approved baselines/measures used to measure progress in terms of cost, schedule, and performance.

**E. Responsibilities:**

1. The Programs and Budget Advisory Committee (PBAC) is co-chaired by the Associate Director for Operations (ADO) and the Associate Director for Administration (ADA), and consists of all of the Assistant Directors (ADs). The role of the PBAC is to make recommendations on courses of action for consideration by the Director and/or Deputy Director as part of the decision-making process. An issue may be sponsored by the ADO, ADA, or any AD, or raised by the District Advisory Working Group (DAWG), but must be approved by the Deputy Director before corporate review and deliberation.

2. The USMS CIO reviews the IT investment portfolio, focusing on major and cross-cutting IT investments that are an integral part of the USMS enterprise architecture. IT Resource Management investment review is integrated into the USMS Configuration Management Board process. The USMS Configuration Management Plan describes the key configuration management activities and practices for the development and operation for all IT systems throughout the SDLC.

3. The USMS CIO conducts Quarterly Program Reviews (QPRs) on IT investments to assess Cost, Schedule, and Performance measures. As directed by the PBAC, and when the USMS CIO deems it appropriate, the USMS CIO conducts independent assessments of USMS IT projects.

**F. Procedures:**

1. The USMS ITD Solution Provider's Guide to the SDLC Management Process complies with federal and departmental requirements and has been approved by the DOJ CIO.

2. United States Marshals Service Configuration Management Plan

**G. Definitions:** None.

**H. References:** None.

**I. Cancellation Clause:** This policy directive supersedes Policy Directive 12.5, *IT Management (ITIM) /System Development Lifecycle (SDLC)*.

**J. Authorization and Date of Approval:**

**By Order of:** **Effective Date:**

/S/ 10/21/12

Stacia A. Hylton
Director
U.S. Marshals Service

## INFORMATION RESOURCES MANAGEMENT

### 12.6 E-GOVERNMENT/WEB MANAGEMENT

**A. Purpose:** This directive provides USMS employees with guidance on the management and maintenance of the USMS Web sites. Districts and Divisions are not authorized to create or manage external public U.S. Marshals Service web site. Content for external USMS web sites is centralized and managed by the Web Manager for the USMS, Information Technology Services. District and division offices may maintain individual Intranet sites as long as the content is consistent with the USMS Intranet procedures and conform to USMS reporting and registration procedures.

**B. Policy:** The USMS Intranet Management Systems have been established to facilitate and further the mission of the USMS and are intended to be used for official government business. Employees should use these sites to share information and resources with one another, to do group work and for teleconferences.

1. **Management:** As delegated by the Chief Information Officer of the United States Marshals Service, the U.S. Marshals Service Web administrator and the Web administration staff maintain the USMS Intranet, provide web management guidance and general guidelines for web content and style, as well as assist district and program offices with their Intranet sites.

2. **District and Program Offices:** For web site records to remain reliable, authentic with integrity, and useable for as long as they are needed, web sites must maintain the content, context, and a coherent structure. Structural information on the organization of the web site supports its long-term integrity. District and division intranet web sites should reflect the following characteristics:

   a. Reliability: A reliable web site is one whose content can be trusted as a full and accurate representation of the transactions, activities, or facts to which it attests and therefore can be depended upon in the course of subsequent transactions or activities.

   b. Security: The web site affords the ability to control the creation, transmission, receipt, and maintenance of web site records to ensure that records creators are authorized and identified and that records are protected against unauthorized addition, unauthorized deletion, and alteration (e.g., via hacking).

   c. Integrity: The integrity of a web site refers to it being complete and unaltered. The structure of a web site, its physical and logical format and the relationships between the pages and content elements comprising the site, should remain physically or logically intact.

   d. Usability: A usable web site is one that can be easily located, retrieved, presented, and interpreted by USMS staff.

e. Authenticity: District or division web sites should contain content that is pertinent to the mission of the district or division office or function. All other content should be hyperlinked to avoid duplication and to ensure the authenticity of content. An authentic web site is one that is proven to be what it purports to be and to have been created by the office that is responsible for the content.

3. **Web-Based Policy and Related Content:** The USMS Policy Center is responsible for managing USMS policy, therefore all references to USMS policy on division and district intranet web sites should contain a link to the official USMS policy web site. Web based USMS Forms and USMS official publications should be hyperlinked to the official USMS Intranet web sites for publications and forms, which is managed by the Management Support Division.

4. **Intranet Search Engines:** To ensure reliable web search queries of all available resources, all intranet sites should utilize the main USMS search engine which is accessible from the USMS home page. Local search engines are not authorized for use.

5. **Registration:** Any office that establishes an intranet web site that is not maintained on an existing, authorized USMS agency web server, must submit an ITIM Configuration Management Request for Change (RFC) to ITS prior to activating the use of a new server and also register it with the USMS Web Administrator. Offices that plan to establish an intranet web site on existing web servers that are managed by ITS are required to register the website with the USMS Web Administrator.

6. **Web Management Contacts:** A contact person must be designated for each site to assist with information management and communication. If the contact person is replaced, an alternate name should be provided to the Web administrator.

7. **Certification:** The contact person for each Intranet site must complete a quarterly certification stating that his or her site meets the criteria outlined in these internal operating procedures. Certifications are due to the Web administrator on the last day of March, June, September and December.

**C. Definitions:**

1. **Intranet:** An intranet is a private network that is contained within an enterprise. It may consist of many interlinked local area networks and also use leased lines in the Wide Area Network.

2. **Web Site:** a collection of information, documents or databases that is provided to a user community using Web formats and protocols; a location managed by a single entity that provides information.

3. **Web Page:** A Web page is an individual computer file that is viewable through a browser and addressed by a hyperlink.

4. **Home Page:** A home page is the entry point to a Web site or a grouping of related pages commonly referred to as a document collection. It is the first page of information received by a visitor to the site or document collection.

5. **Content:** The actual html, XML or otherwise encoded pages and additional content files referenced therein (or graphic files produced by other); records that are created dynamically in real time when a user interacts with an agency web site (e.g., on-the-fly, text-based page creation, forms filled out online, etc.); files having the ability to 'self-execute' (e.g., CGI scripts, Java/ActiveX applets, customized programs that generate on-

line sound or moving images) as well as files that are static (e.g., these include graphic files, multi-national character sets, etc.), both external to the HTML-encoded content pages but referenced in the HTML syntax;

6. **Document:** A document is information designed to be read and presented as a discrete entity. An electronic version can be either read through a browser or downloaded for later use.

7. **Browser:** A browser is a program for reading hypertext. Since this is the primary function of a Web client, they are generally called browsers. Common browsers include Mosaic, Netscape, Microsoft Internet Explorer and Lynx.

8. **Hypertext:** This is text that contains links to other documents, can be chosen by a reader, and causes another document to be retrieved and displayed.

9. **Hyperlink:** highlighted text or images that contain links to other information or documents.

10. **Downloadable File:** A computer file that is not intended to be viewed by a browser, a downloadable file can be addressed by a hypertext link. Additional software may be required to access the file.

Additional definitions can be found in the Glossary of Terms for the DOJ, Web Content Guidelines, May 1999.

**D. Appendices:**

***Appendix 12.6A: Intranet Website Design and Usability Guidance***

***Appendix 12.6B: Intranet Web Certification Form***

***Appendix 12.6C: USMS Request to Access Blocked Internet Web Site***

United States Marshals Service POLICY DIRECTIVES

## INFORMATION TECHNOLOGY

### 12.7 Information Technology (IT) Security

**A.** **Proponent:** Chief Information Officer (CIO), Assistant Director for Information Technology Division (ITD), Telephone: 202-307-5414.

**B.** **Purpose:** To establish responsibilities, authorities, and guidance for the protection and secure management and operation of United States Marshals Service (USMS) IT systems which store, process, or transmit classified and unclassified information. This policy applies to all persons who use USMS IT resources including, but not limited to, employees, contractors, task force officers, and interns. This policy applies to classified and unclassified computer and telecommunications resources systems, and peripheral devices that are acquired for use by, owned, operated, or managed by the USMS.

**C.** **Authority:** Department of Justice (DOJ) Order 2880.1B, *Information Resource Management Program*; DOJ Order 2640.2F, *Information Technology Security;* DOJ Order 2420.2, *Telecommunications Policy and Guidelines*; DOJ Order 2740.1A, *Use and Monitoring of DOJ Computers and Computer Systems*; DOJ 2421.1E, *Use of Government Telecommunications Systems*; DOJ Certification & Accreditation Handbook, May 2009; Policy Directive 1.1, *Delegation of Authority, Organization and Functions*; Policy Directive 12.1, *Information Resources and Technology Management*; OMB Memorandum M-08-05; OMB Circular A-130 Appendix III, *Security of Federal Automated Information Systems*; Federal Information Security Management Act (FISMA); National Institute of Standards and Technology (NIST) *Recommended Security Controls for Federal Information Systems and Organizations*, NIST Special Publications 800-53; and the DOJ IT Control Standards as amended:

1. 1.6 Classified Laptop and Standalone Computers (Version 2.1), November 2006;
2. Access Control (Version 2.2), June 2008;
3. Audit and Accountability (Version 2.1), June 2008;
4. Awareness and Training (Version 3.1), June 2008;
5. Certification, Accreditation, and Security Assessments (Version 3.2), June 2008;
6. Configuration Management (Version 1.1), June 2008;
7. Contingency Planning (Version 2.1), June 2008;
8. Identification and Authentication (Version 2.1), June 2008;
9. Incident Response (Version 3.0), February 2009;
10. Maintenance (Version 2.0), December 2006;
11. Media Protection (Version 3.1), June 2008;
12. Personnel Security (Version 3.2), June 2009;
13. Physical and Environmental Protection (Version 3.1), June 2008;
14. Planning (Version 3.2), June 2008;
15. Risk Assessment (Version 3.1), June 2008;
16. System and Communications Protection (Version 1.1), June 2008;
17. System and Information Integrity (Version 2.0), December 2006; and
18. System and Services Acquisition (Version 3.1), June 2008.

**D.** **Policy:** This policy applies to all persons who use USMS IT resources including, but not limited to, employees, contractors, task force officers, and interns. This policy applies to classified and

unclassified computer and telecommunications resources, systems, and peripheral devices that are acquired for use by, owned, operated, or managed by the USMS. The USMS is responsible for maintaining an IT security program to ensure the confidentiality, integrity, and availability of the USMS computer systems, networks, and data. IT security policy is organized in accordance with the NIST *Recommended Security Controls for Federal Information Systems and Organizations*, NIST Special Publications 800-53, and the DOJ IT Control Standards as amended:

1. **New IT Systems:** All new IT systems must comply with applicable IT security requirements and DOJ standards prior to being authorized for production.

2. **Existing IT Systems:**

   a. IT Systems that meet all DOJ requirements, but do not meet all USMS requirements as set forth in this policy and related procedures: The program office that has been using the non-compliant system must request a written waiver from the Assistant Director for ITD. The waiver must:

      1) Indicate how the IT system deviates from IT security policy or procedures;

      2) Provide a general plan on how the IT system will become compliant with the policy or procedure; and

      3) Indicate how the IT system will mitigate any inherent IT security risks.

   b. IT Systems that do not meet all DOJ requirements as set forth in the DOJ IT System Security (ITSS) standards*:* The program office that has been using the non-compliant systems must work with ITD to submit a waiver request to the DOJ CIO. The specific instructions for requesting a waiver are outlined in accordance with ITSS standards.

3. **IT Security Management Policy:** The IT security management strategy and policy are based on risk management concepts and principles. An important factor in effectively implementing these principles is linking them in a cycle that ensures IT security policy addresses current risks on an ongoing basis.

   a. **Central Focal Point:** The CIO and, as delegated by the CIO, the Deputy Assistant Director for ITD, the Chief Technology Officer (CTO), and the Chief Information Security Officer (CISO) are the principal managers responsible for the management of IT security and IT security strategy in the USMS.

      1) ITD assumes a leadership role with USMS divisions in managing the agency priorities for achieving business objectives and complying with federal and DOJ IT security requirements.

      2) ITD coordinates IT security planning and oversight with the USMS Security Programs Manager (SPM), Office of Security Programs, Tactical Operations Division (TOD).

   b. **Common Security Strategy:** Users of IT resources and services will follow common security strategy, developed by the CIO, that follows common security goals for all mission requirements. The common security strategy strengthens the maintenance of

a common IT security architecture and ensures that information systems remain secure throughout their lifecycle. The security needs and requirements shall be identified early on in the process and funded appropriately.

c. **New and Emerging Technologies:** Division and district offices will coordinate all evaluation plans for new IT technology with the CIO and CTO prior to utilizing new or emerging technologies. The CIO and delegated staff will maintain all evaluation plans of
new or emerging technologies.

d. **Manage IT Security Risk and Determine Needs:** ITD is responsible for conducting periodic assessments of risk to agency operations, assets, individuals, and other organizations resulting from the operation of USMS IT systems and the associated
processing, storage, or transmission of information.

1) The CIO is responsible for the development and management of a formal, structured approach for developing risk assessments for IT systems that are part of a major application or general support system. This responsibility can be delegated by the CIO to specific ITD staff.

2) ITD is responsible for establishing formal, documented procedures to facilitate the implementation of risk assessment controls of IT systems.

3) Based on a thorough examination of risks, USMS managers are responsible for operating IT systems based on risks identified in formal assessments balanced by the impact an IT system has on USMS operations.

e. **Planning:** ITD is responsible for developing, documenting, disseminating, periodically updating, and implementing security policy, plans, and procedures for IT systems, as well as the rules of behavior for individuals accessing the IT systems.

f. **System and Services Acquisition:** ITD, through collaborative planning with USMS executive management, is responsible for:

1) Allocating sufficient resources to adequately protect DOJ IT systems;

2) Employing systems development life-cycle processes and procedures that incorporate IT security considerations;

3) Ensuring new IT system acquisitions include available standard security configurations;

4) Ensuring third party providers are contractually required to comply with USMS policy to employ adequate security measures to protect information, applications, and services outsourced from the USMS; and

5) Employing software usage and installation restrictions to ensure software installed on USMS systems and workstations is in compliance with applicable copyright laws and licensing agreements.

g. **Certification, Accreditation, and Security Assessments:** ITD is responsible for establishing plans, procedures, and IT system monitoring controls to certify,

accredit, and assess the security of IT systems and network connections between IT systems.

h. **Interconnection Agreements:** ITD is responsible for authorizing all connections from USMS information systems to other information systems outside of the accreditation boundary, as well as for monitoring/controlling the system interconnections on an ongoing basis. The CIO is the approving official for USMS information system interconnection agreements.

i. **Accreditation:** The CIO, or delegated ITD staff, have approval and signatory authority for accrediting IT systems prior to their functioning or processing information, and are responsible for updating the authorization every three years and/or whenever there is a major change.

j. **Classified Systems:** The CIO, in collaboration with the Assistant Director for TOD and the Assistant Director for the Witness Security Division (WSD), is responsible for the security, administration, and management of classified information, and is responsible for ensuring that classified IT systems comply with specific requirements found in the DOJ Security Program Operating Manual (SPOM), federal requirements for national security systems, and instructions published by the Committee on National Security Systems (CNSS).

4. **The CIO is responsible for:**

a. Implementing the IT security program;

b. Establishing a USMS organizational risk management capability of monitoring, testing, and evaluating the effectiveness of IT security policy, procedures, practices, and security controls;

c. Issuing IT security policy, standards, and guidelines;

d. Developing and managing IT control techniques, technologies, and enterprise management tools;

e. Developing and maintaining the IT security program management plan (PMP) in accordance with federal and DOJ regulations;

f. Developing, implementing, and managing an agency Plan of Action and Milestone (POAM) process consistent with DOJ guidance to correct IT security weaknesses;

g. Integrating security in the Capital Planning Investment Control (CPIC) process;

h. Reporting on the status of IT security programs to the DOJ CIO and CISO;

i. Assigning IT security roles and responsibilities within the USMS;

j. Coordinating with the DOJ Office of the CIO (OCIO) any evaluations of new technologies that could impact DOJ enterprise services;

k. Participating with other DOJ components and the OCIO in evaluating and selecting IT security tools for use within DOJ and obtaining DOJ CIO approval for non-enterprise IT security solutions;

l. Establishing procedures to ensure software installed on IT systems is in compliance with applicable copyright laws and is incorporated into the IT system's lifecycle management process;

m. Approving, with the concurrence of the DOJ CIO and DOJ Security Officer (DSO), and monitoring waivers relating to non-United States citizens who access or assist in the development, operation, management, or maintenance of DOJ IT systems;

n. Ensuring all USMS personnel with access to DOJ networks and all individuals at contractor facilities working on USMS or DOJ systems information, or providing services, receive annual IT security awareness training; and

o. Ensuring USMS executive management provides IT security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained
by, or on behalf of the USMS and/or IT systems used or operated on behalf of the USMS.

5. **Designated Accrediting Authority (DAA):** The DAA is a senior management official within the USMS, responsible for operating a USMS information system and related IT assets. The DAA is appointed by the CIO for non-intelligence community information systems. The DAA is responsible and accountable for:

a. The oversight of the budget and business operations of the system within the USMS;

b. The approval of system security requirements, System Security Plans (SSPs), and memorandums of agreement (MOA), and/or memorandums of understanding (MOU);

c. The risks associated with operating a system through security accreditation process;

d. Issuing the Authorization to Operate (ATO) USMS information systems;

e. The issuance of an ATO under specific terms and conditions; and

f. Issuing denials of an ATO for the information system, or halting system operations if there are unacceptable security risks.

6. **CISO:** The CISO is the principal security leader for the USMS for implementing the requirements of FISMA. The CISO also is the CIO's liaison to DOJ for matters relating to implementation of the DOJ IT security program. The CISO is responsible for:

a. Ensuring computer systems in the USMS are operated in accordance with the federal and departmental standards and requirements related to the Information Security Management Act of 2002, NIST *Recommended Security Controls for Federal Information Systems and Organizations*, NIST Special Publications 800-53; and DOJ requirements;

b. Ensuring requests for new computer systems, or changes to existing systems, include appropriate security requirements, and that these requirements are incorporated into the system design;

c. Promulgating telecommunications and automated information systems security guidance within USMS, to include developing USMS specific guidance as required;

d. Ensuring security plans are prepared for all computer systems under his/her authority which process sensitive or classified information;

e. Maintaining a record system containing the status of all Certification and Accreditation (C&A) documentation;

f. Reporting immediately to the CIO any security violation, attempt to gain unauthorized access to information, virus infection, or other event affecting the security of the computer systems; and

g. Serving as the Chair of the Change Control Board (CCB) to ensure configuration management for security-relevant system software, hardware, and firmware is maintained and documented.

7. **Information System Security Officer (ISSO):** The ISSO is the component official assigned by the DAA or management official for ensuring that the appropriate operational security posture is maintained for an information system or program. The ISSO is responsible for:

a. Assisting the CISO in the identification, implementation, and assessment of the common security controls;

b. Assisting in developing and updating the SSP, and coordinating with the information system owner, any changes to the system and assessing the security impact of those changes;

c. Ensuring systems are operated, maintained, and disposed of in accordance with security policies and practices outlined in the approved accreditation package;

d. Reporting all security-related incidents to the CISO;

e. Initiating, with the approval of the CISO, protective and corrective measures when a security incident or vulnerability is discovered;

f. Monitoring system recovery processes to ensure the proper restoration of system security features;

g. Performing self-assessments, on an annual basis at minimum, to ensure compliance with the SSP;

h. Serving as a member of the CCB to ensure configuration management for security-relevant system software, hardware, and firmware is maintained and documented;

i. Ensuring system security requirements are addressed during all phases of the system's lifecycle;

j. Establishing audit trails, ensuring their review, and making them available when required by the CISO;

k. Retaining audit logs in accordance with DOJ and USMS policy; and

l. Ensuring awareness and precautionary measures are exercised to prevent introduction and/or proliferation of malicious code.

8. **IT Operational Security Policy:** Operational security policy and related controls are the safeguards or countermeasures for an information system that are primarily implemented and executed by people, as opposed to IT systems.

a. **Awareness and Training:** ITD is responsible for ensuring and documenting that all USMS IT system and network users, including managers and senior executives, are exposed to basic information system security awareness training and related materials on an annual basis.

b. **Configuration Management:** ITD is responsible for:

1) Documenting, reviewing, and updating IT configuration management policy, procedures, and plans for IT systems;

2) Maintaining baseline configurations and change management processes for IT systems and computer workstations;

3) Establishing and maintaining configuration documentation; and

4) Ensuring appropriate USMS officials approve information system changes in accordance with component policies and procedures.

c. **Contingency Planning:** ITD is responsible for:

1) Coordinating contingency planning and testing for IT systems, data storage, and recovery;

2) Developing and implementing an IT contingency plan for information systems;

3) Providing annual training for USMS personnel associated with IT system contingency roles and responsibilities with respect to USMS information systems.

d. **Alternative IT Storage and Data Processing:** The CIO, in collaboration with USMS executive management, is responsible for:

1) Identifying an alternate storage and data processing site; and

2) Initiating necessary agreements to permit the storage of information for IT system backup, and permit the resumption of information system operations for critical mission/business functions within a component-defined time period when the primary processing capabilities are unavailable.

e. **Alternative IT Storage of Digital Imagery:** The Assistant Director for TOD is responsible for the management of digital imagery captured by headquarters facility security systems.

f. The Assistant Director for the Management Support Division (MSD) is responsible for infrastructural elements of security for alternative IT storage and data processing facilities that reside in USMS owned or leased space.

g. **Telecommunications:** The CIO, in collaboration with USMS executive management, is responsible for:

1) Identifying primary and alternate telecommunications services to support USMS information systems; and

2) Initiating necessary agreements to permit the resumption of system operations for critical mission/business functions within component-defined time period when the primary telecommunications capabilities are unavailable.

h. **Secure Telecommunications Systems:** The Assistant Director for TOD is responsible for the secure telecommunications within the USMS.

i. **Incident Response:** The CIO and delegated ITD staff are responsible for:

1) Developing, disseminating, and updating a formal, documented computer incident response policy and procedures that address the scope, roles, and responsibilities to facilitate the implementation of a plan consistent with the DOJ Incident response Plan (IRP); and

2) Managing IT incident response training and testing.

j. **IT Security Incidents:** The CIO and ITD delegated staff are responsible for implementing a USMS incident handling capability for security incidents, including preparation, detection and analysis, containment, eradication, and recovery of IT systems and information.

k. **IT Maintenance:** ITD is responsible for:

1) The oversight and general management of routine preventative and regular maintenance on the components of the IT systems in accordance with manufacturer or vendor specifications and/or organizational requirements;

2) The use of the information system maintenance tools and the management of personnel authorized to perform maintenance on USMS information systems; and

3) Authorizing, in conjunction with the Human Resources Division (HRD), personnel to perform maintenance on USMS information systems.

l. **Media Protection:** ITD, in collaboration with the Office of Security Programs, TOD, is responsible for establishing procedures and guidance on IT Media protection, access, labeling, storage, transport, and sanitization and disposal practices within the USMS.

m. **Physical and Environmental Protection:** For specific locations within a USMS facility or contract facility containing concentrations of USMS information system resources (e.g., data centers, server rooms, mainframe rooms), the CIO, in collaboration with the Assistant Director for MSD, is responsible for the development, management, and oversight of procedures and security controls for physical access authorizations, physical access control, visitor control, access to IT records, and infrastructure resources (e.g., emergency power, emergency lighting, fire protection, temperature and humidity controls, water damage).

n. **Personnel Security:** ITD is responsible for:

1) Establishing and managing security controls associated with IT user accounts;

2) Ensuring adequate controls are in place to ensure USMS personnel have access to information commensurate with mission requirements and security clearance levels; and

3) Establishing personnel security requirements for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management) and monitoring provider compliance to ensure adequate security.

o. **System and Information Integrity:** ITD is responsible for:

1) Establishing and managing IT security controls that identify, report, and correct information system flaws, implement malicious code protection that includes a capability for automatic updates, employ malicious code (e.g., viruses, worms, Trojan Horses) detection and eradication mechanisms on all systems (e.g., firewalls, servers, workstations, mobile computing devices, applications) for which such protection mechanisms are available;

2) Employing tools and techniques to monitor events on the information system and to detect attacks and provide identification of unauthorized use of the system;

3) Coordinating IT security alerts and advisories;

4) Performing self-tests to verify the correct operation of security functions as defined in the SSP; and

5) Instituting control mechanisms to protect against unauthorized changes to software and information.

9. **Technical Security Policy:** Technical security policy and related controls are the safeguards or countermeasures for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

a. **Access Controls:** ITD is responsible for:

1) Management of information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts, performing annual reviews of IT system accounts, and instituting adequate system controls for controlling access to the system in accordance with applicable policies;

2) Managing information flow enforcement practices within and between systems; and

3) Establishing policies and procedures governing the remote access of government or contractor-owned systems that manage USMS information.

b. **Audit and Accountability:** ITD is responsible for:

1) Establishing and managing IT system auditing capabilities and controls that generate audit records for specific events;

2) Establishing systems to track and audit specific individual user actions and contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events within an IT system;

3) Providing the technical capability for the regular review and analysis of audit records for indications of inappropriate or unusual activity; and

4) Investigating suspicious IT activity or suspected violations and reporting findings to appropriate officials.

c. **Identification and Authentication:** ITD is responsible for instituting technical controls for IT systems that uniquely identify and authenticate users (or processes acting on behalf of users) of IT systems.

d. **Information Management Authenticators:** In collaboration with MSD and TOD, ITD is responsible for managing information system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by:

1) Defining initial authenticator content;

2) Establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators; and

3) Revoking authenticators; and changing default authenticators upon information system installation.

e. **System and Communications Protection:** ITD is responsible for maintaining IT technical security controls that effectively monitor and protect IT network and wireless communications and IT systems.

1) All connections to external networks supporting external access and/or remote access to USMS, DOJ, federal, state or local systems are obtained through a Trusted Internet Connection Access Provider (TICAP), unless the USMS and DOJ CIO grant a waiver based on assessed risk, mitigation controls, and operational requirements.

2) ITD is responsible for establishing policy and procedures governing remote access processes that employ approved cryptographic mechanisms or protected distribution systems, and managing IT resources for blocking external malicious resources and internet sites.

3) ITD is responsible for establishing policy and procedures for the use of VPN connections for remote access to IT systems.

4) ITD is responsible for establishing usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system (including Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript).

**E. Procedures:** The procedures associated with IT security have been organized in accordance with the basic categories of IT security control areas contained in NIST *Recommended Security Controls for Federal Information Systems and Organizations*, NIST Special Publications 800-53;

and the DOJ IT Control Standards as amended: This information is provided in separate appendices or separate documents.

1. **Management Controls:**

   a. **Security Assessment and Authorization:** Accreditation of each IT system must be performed at least every three years, or whenever there is a significant change to the system, or a breach of security. Refer to Appendix 1, Security Assessment and *Authorization,* for separate procedures for the implementation of the Security Assessment and Authorization program within the USMS.

   b. **Planning:** The planning procedures in the IT security program define specific issues that need to be addressed in the development of new IT systems, the design of new segments or phases of a system, or in the triennial review of the systems. Refer to Appendix 2, *IT Security Planning,* for separate procedures for the use of these documents.

   c. **Risk Assessment:** Formal IT security risk assessments are performed on all IT systems. Assessments are performed at the inception of a new system. Once a system has been certified and accredited, an annual review of the risk assessment will be completed in conjunction with the review of the SSP and any relevant **Plan of Action** and Milestones (POA&M) for the system. The information system's risk assessment must be updated whenever there is a significant change to the system or other conditions impact the security of the system. Refer to Appendix 3, *Risk Assessment,* for separate procedures for the completion of risk assessments within the USMS. Refer to the Vulnerability Management Program.

   d. **System and Services Acquisition:**

      1) Procedures associated with IT system and services acquisition are guided by the IT Investment Management (ITIM) process and the System Development Life Cycle (SDLC). Refer to Policy Directive 12.5, *IT Investment Management* (ITIM), and the Solution Provider's Guide to the SDLC.

      2) **Request for Change Procedures:** The request for change process provides guidance when requesting changes to existing IT systems, whether the change is as routine as replacing a broken object within a system, or as complex as initiating the development of an entirely new application. This Request for Change (RFC) process must involve the requesting program office as well as various IT staffs to ensure that the business requirements are adequately defined and all potential technical solutions are considered and reviewed for the security implications for the agency. Refer to the Configuration Management Plan (CMP).

2. **Operational Controls:**

   a. **Awareness and Training:** Users will participate in the annual Computer Security Awareness Training (CSAT). ITD staff will comply with identified security training relevant to their job functions. Failure to comply with mandatory computer security awareness or specialized training may result in the loss of access to IT systems. Refer to Appendix 4, *Awareness and Training,* for separate procedures for additional information on awareness or advanced levels of security training.

b. **Configuration Management:** Configuration management is the process by which USMS IT managers are assured that the initial deployment of IT hardware and software has been completed in the most secure manner possible. The establishment of baseline configurations for security profiles should include inventories of the information system (including hardware, software, and firmware), and all documentation that is generated throughout the SDLC process. Refer to Appendix 5, *Configuration Management,* for separate procedures for additional information on configuration management. Refer to the CMP.

c. **Contingency Planning:** It is the responsibility of every USMS organizational component to protect life and property by maintaining an effective Occupant Emergency Plan (OEP) in each USMS building or facility throughout the United States. Refer to Appendix 6, *Contingency Planning,* for additional information on contingency planning for IT systems.

d. **Computer Incident Response:** It is the responsibility of ITD to monitor the general IT environment of the USMS to protect against unauthorized access, particularly from outside threats. It is the responsibility of every IT user to be aware of situations that might indicate a threat against the agency's IT resources and to report that potential problem to the proper authorities. The general point of contact for any IT emergency is the IT Helpdesk at 202-307-5200. Refer to Appendix 7, *Incident Response,* for additional information on incident response requirements and procedures. Refer to the Computer Incident Response Plan (CIRP).

e. **Maintenance:**

1) Maintenance for hardware will be provided through warranty provisions or contracts for appropriate support, defined by the business requirements of the applications being hosted by the hardware.

2) Software maintenance contracts will be used where it is economically feasible to support the applications in use on the specific equipment.

3) Enterprise Licensing Agreements will be used to the extent possible to provide the most economical way of obtaining licenses and maintenance contracts.

4) Only USMS personnel or personnel under contract to the USMS may perform hardware and software maintenance. Contractors must have USMS clearance, or be escorted at all times by a person who can be reasonably expected to understand the general work that the contractor is performing. Persons who come on-site to perform maintenance functions will be required to sign in and be escorted by USMS personnel with existing clearances. Refer to Policy Directive 12.3, *User Access to USMS IT User Systems,* and Standard Operating Procedures: Account Management.

f. **Media Protection:** The exact methods for controlling and marking the media will be contingent on the type of device, and the technical solutions available at the time the media is in use. Refer to Appendix 8, *Media Protection,* for additional information on media controls and proper marking.

g. **Physical and Environmental Protection:** USMS staff are to adhere to specific physical and environmental security procedures and controls that directly relate

to the protection of all IT systems, including user workstations, as well as USMS computer centers, computer rooms, and telephone (voice and data) circuits and access rooms (also known as telephone closets). Refer to Appendix 9, *Physical and Environmental Protection,* for additional information on physical and environmental protection instructions.

h. **Personnel Security:** Within the IT security program, the term "personnel" includes all users of IT systems.

1) Any user must have received the appropriate approval by the office of Background Investigations (BI) prior to receiving access to any USMS information system.

2) The request for access to the IT systems must be completed by the user's office through the form USM-169, *User Account Request (UAR).*

3) The requesting office must verify that the proper approval has been received from the BI office, that the user has been informed of the general Rules of Behavior (ROB), and that the access being requested includes only access that is required to perform the duties of the job.

4) The user and the supervisor must work with ITD to ensure that appropriate segregation of duties is maintained within each IT system.

5) The office is responsible for submitting a USM-169 to terminate the user's access when specific system access is no longer needed, and/or when the user leaves the USMS. Refer to Appendix 10, *Personal Security,* for additional information on IT Personal Security and also Standard Operating Procedures: Account Management.

i. **System and Information Integrity:**

1) ITD is responsible for providing virus detection tools and procedures that are applied throughout the entire agency and ensuring that operating system and application patches are applied in a timely manner throughout the entire agency.

2) End users are required to report any incident that they think might involve a breach in the security of the IT systems, and include reports of possible viruses on their assigned equipment. Users may not disable the anti-virus systems on their assigned equipment, and must follow prescribed procedures to enable automated uploads of virus definitions files and patches, and automated scans of their systems. Refer to Appendix 11, *System and Information Integrity,* for additional information on virus detection, anti-virus guidelines, vulnerability scanning, and patch management.

3. **Technical Controls:**

a. **Access Controls:** The logical access controls are maintained by ITD so that access to information systems is limited to authorized users, processes acting on behalf of authorized users, or devices limited to the types of transactions and functions that authorized users are permitted to perform.

1) Although users must have access to perform their jobs; they must also be denied access to non-job related functions.

2) ITD uses logical access controls built into the operating system, incorporated into applications programs and major utilities, as well as those that can be implemented through add-on security packages.

3) Access controls include account locking procedures for work stations when not in actual use, and for end user or system administrator accounts that have not been used within prescribed periods of time.

4) Controls for remote access must comply with DOJ requirements, and utilize the DOJ provided Justice Secure Remote Access (JSRA).

5) No workstations are allowed to have active network access (MNET LAN) at the same time as any other active WAN connection, including telephone modems, cable modems, DSL connection, or any wireless connection. Refer to Appendix 12, *Access Controls,* for additional information on account locking, remote access, and external, internal, and wireless communications.

b. **Audit and Accountability:** The technical controls for system auditing and accountability are implemented by specific sections of ITD, with the review of the audit logs performed by other assigned sections of ITD. Refer to Appendix 13, *Audit Accountability,* for additional information on system auditing and audit accountability. Refer to Standard Operating Procedures for System and User Activity Audit Logging.

c. **Identification and Authentication:** All IT systems are required to incorporate both user identification (userid) and user authentication (passwords). The combination of userid and password must be unique for each user.

1) Each user is required to have a unique userid logon. Minimum requirements and standard conventions for passwords are established by DOJ.

2) USMS users are encouraged to use the strongest possible passwords in each system. As of December 1, 2008, the minimum requirements for user passwords are: (1) Maximum Duration – 60 days; (2) Minimum Length – 12 characters; (3) Composition – Passwords must contain characters from at least three of the four character sets (uppercase letters, lowercase letters, numerals, and special characters); (4) Inactivity Lock – after 20 minutes of no use; and (5) Recycling Limitation – cannot repeat for 24 cycles. Refer to Appendix 14, *Identification and Authentication,* for additional information on identification and authentication.

d. **System and Communications Protection:** The USMS uses a variety of technologies to accomplish this protection, and relies on the DOJ Unified Telecommunications Network (JUTNet) to provide the first level of protection for all communications that exit spaces physically controlled by the USMS. Refer to Appendix 15, *Systems and Communications Protection,* for additional information.

**F. Classified Laptop and Mobile Computing Devices:** The DOJ DSO and DOJ CIO shall approve, in writing, the processing of classified information on laptops and mobile computing devices. Requests for approval shall be submitted through the CISO who will obtain the approvals. DOJ IT Security Standard – Classified Laptop and Standalone Computers Security

Policy outlines the requirements for laptop computers that process or store classified information, including requirements for standalone computers that process or store classified information.

**G. Use of IT Resources Outside United States Territory:** The DOJ DSO and DOJ CIO provide written approval for the transportation or use of DOJ computers outside of United States Territory. The USMS CIO is the approval authority for the use of telephones, including BlackBerry smart phones and similar devices, outside United States Territory. USMS offices and staff shall:

1. Limit data taken outside United States Territory to that which is needed to accomplish the purpose of the travel.

2. Prevent remote access to USMS and DOJ IT systems from outside United States Territory, with the exception of systems specifically accredited for such access and email via smartphones or personal digital assistants (PDAs).

3. Inspect computers, smart phones, PDAs and media that have been transported outside United States Territory for compromise prior to any physical connection to a USMS or DOJ system. If the component can not conduct such an inspection, appropriate staff shall reimage the computer or sanitize the media.

**H. Facsimile:**

1. All classified and sensitive facsimile transmissions shall be preceded by a cover sheet containing the following information:

   a. The classification or sensitivity of the information;

   b. The name, office, and, voice/fax telephone numbers for the recipient(s) and sender; and

   c. A warning banner with instructions to the recipient if the facsimile was received in error.

2. Classified information shall be encrypted for transmission with National Security Agency (NSA)-approved encryption.

**I. Sensitive and Personally Identifiable Information (PII):** It is the objective of the USMS to support policies that compensate for the lack of physical security controls when information is removed from or accessed from outside the agency location. Refer to Appendix 16, *PII.* USMS staff shall:

1. Reduce the volume of collected and retained PII to the minimum necessary;

2. Limit access to only those individuals who must have such access;

3. Categorize sensitive PII and information systems processing such information as moderate or high impact;

4. Not remove sensitive PII from USMS controlled IT systems or facilities unless required (e.g., court filings and debt collection activities);

5. Log all computer-readable data extracts from databases holding sensitive information and ensure each extract including sensitive data has been erased within 90 days or its use is still required. All DOJ information is considered sensitive information unless designated as non-sensitive by the Director of the USMS; and

6. Ensure all contracts involving the processing and storage of PII comply with DOJ policies on remote access and security incident reporting.

**J. External Information Systems:** External information systems are information systems that are outside of the accreditation boundary established by the USMS, and for which the USMS typically has no direct control over the application of required security controls or the assessment of security control effectiveness. External access includes interconnections between DOJ IT systems and non-DOJ IT systems, and between IT systems internal to the DOJ, where there is direct connection of two or more IT systems for the purpose of sharing data and other information resources. External access also includes connections to the Internet. USMS divisions, districts, and other USMS offices shall:

1. Obtain all connections to external networks that support external access and/or remote access through a TICAP, unless the USMS CIO and DOJ CIO grant a waiver based upon assessed risk, mitigation controls, and operational requirements; and

2. Be prohibited from deploying systems, technologies, or services (e.g., encapsulation, tunneling, and encryption) inconsistent with department security architecture requirements (e.g., firewalls, intrusion detection or prevention systems, antivirus systems, content scanning and filtering systems), unless the USMS CIO and DOJ CIO grants a waiver based upon assessed risk, mitigating controls, and operational requirements prior to operational use.

**K. Protection of Mobile Computers/Devices and Removable Media:** Information physically transported outside of the USMS's secured physical perimeter is more vulnerable to compromise. The intent of this policy is to compensate for the protections no longer offered by the physical security controls when information is removed from a USMS location.

1. Information on mobile computers/devices (e.g., notebook computers, PDAs) and removable media shall be encrypted using FIPS 140-2 validated or NSA-approved encryption mechanism, based on the classification of information processed on the device; unless the data is determined to be non-sensitive, in writing, by the USMS Director or Deputy Director.

2. Mobile computers shall utilize anti-viral software and a host-based firewall mechanism. Components shall ensure all security related updates are installed on mobile computers/devices.

3. Information should be deleted from mobile computers/devices when no longer needed.

**L. Remote Access to USMS and DOJ Systems:** Remote access to USMS and DOJ systems is authorized under specific conditions and computer and network configurations, as specified in Policy Directive 12.2, *The Management, Use, Allocation, Deployment, and Accountability, of United States Marshals Service (USMS) Information Technology (IT) Resources and System*.

**M. Contractors:** Contractors can be utilized to develop, operate, and/or maintain IT systems on behalf of the USMS. Contractors may be granted access to IT systems and information in order to perform work specified under the contract.

1. Access may be from USMS-owned computers.

2. Contractors may not process USMS information on contractor owned equipment, either within or outside DOJ space. In all these situations, the contractors and their sub-contractors, their personnel, and their IT systems and devices shall fall under the provisions of this order, and the contract shall identify IT security requirements.

3. All connections to external networks supporting access to DOJ hosted resources (e.g., government-owned web sites, applications, email systems) shall be obtained through a TICAP, unless the DOJ CIO grants a waiver based upon assessed risk, mitigation controls and operational requirements.

4. When the contract requires or allows contractor IT systems to be used, whether to access USMS or DOJ IT systems and/or information or to process or store USMS or DOJ information, the contract shall require the contractor IT systems be certified, accredited, and operated pursuant to a valid ATO. The ATO shall be issued by a USMS Authorizing Official. If the contractor utilizes its own internal C&A process, it must submit the C&A package to the Component Authorizing Official. If the Component Authorizing Official determines the C&A process meets the DOJ standards, he or she may issue an ATO based on the C&A package.

5. Contractors using individual devices under the contract shall provide the Contracting Officer's Technical Representative (COTR) an inventory of such devices and shall operate such devices pursuant to this policy, including all incident response requirements. Contractors and contractor systems shall be subject to the same FISMA data calls as other DOJ systems.

6. Upon termination of contract work, all DOJ information shall be removed from contractor-owned IT equipment. Certification of data removal shall be performed by the contract's project manager and a letter confirming certification shall be delivered to the Contracting Officer within 15 days of the termination of the contract.

**N. Definitions:** Terms used in this policy have the meaning defined by National Institute of Standards and Technology Interagency Reports (NISTIRs), Federal Information Processing Standards (FIPS) and Special Publications (SP). Unless otherwise stated, all terms used in NIST publications are also consistent with the definitions contained in the Committee on National Security Systems Instruction No. 4009, National Information Assurance Glossary.

**O. Cancellation Clause:** Supersedes USMS Policy Directive 12.7, *Information Technology (IT) Security.*

**P. Authorization Date and Approval:**

**By Order of:** **Effective Date:**

/S/ 03/22/2010

John F. Clark
Director
U.S. Marshals Service

## 12.7.1 USMS IT Security Procedures

These procedures, standards, and guidance implement policy contained in USMS Directive 12.7 and have been organized in accordance with the basic categories of IT Security contained in National Institute of Standards and Technology (NIST) Special Publications 800-26 and 800-53, and the Department of Justice (DOJ), *Information Technology Security Staff (ITSS) Standards*.

### A. Risk Management:

1. In accordance with sound business practices and all appropriate federal laws and regulations, the USMS will evaluate the threats to all USMS IT systems to analyze the impact of the loss of the system or its data, and to integrate the needs of USMS program offices (mission areas) in the assessment of the risk. In those cases in which it is possible to reliably predict the cost of a threat or exploitation of a vulnerability, qualitative evaluations will be made. In all other cases, the risk will be evaluated based on the predicted impact of the loss of the system.

2. Risk management is an essential part of the Certification and Accreditation (C&A) process. Once a system has been certified and accredited, an annual review of the risk assessment will be completed in conjunction with the review of the System Security Plan and any relevant Plans of Action and Milestones for the system.

3. The risk assessment at the time of the Accreditation will be considered the baseline security configuration for the system. Documentation of this baseline will be maintained by the Information System Security Officer (ISSO) for the system, with copies kept in the C&A package.

4. The formal risk assessment will produce a list of possible threat sources and known system vulnerabilities. This information will also be maintained by the ISSO and the C&A documentation.

*Additional References:* For further information, refer to Department of Justice, *Information Technology Security (ITS) Standard 1.1 Risk Management* (Version 1.0), dated January 30, 2004.

### B. Review of Security Controls:

1. **General:** In addition to providing the documentation that management needs to be assured that all IT systems are operating in the most secure manner possible, all USMS IT systems must be certified and accredited prior to full deployment (see Section 4 for specific details on the C&A process. A significant outcome of the C&A process is the production of the information needed to allow USMS information systems to connect to each other. This information also provides the framework for determining if USMS systems can be interconnected to external information systems. To this end, the establishment of baseline configurations for security profiles and rigid control of changes

to all systems is an essential feature of the management controls in the USMS computer security program.

2. **Sensitive But Unclassified (SBU) Systems:** Unless specifically exempted from this requirement, all USMS SBU information systems will operate over one agency network – the Marshals Network (MNET) – and over one office automation platform – the USMS deployment of the Justice Consolidated Office Automation Network (JCON).

3. **Classified Systems:** Information about the classified systems will be maintained in accordance with the security guide for the applicable system.

4. **External User Access to USMS IT Systems:** Non-USMS personnel (e.g., state/local law enforcement entities needing access to WIN data, or court/attorney personnel needing access to PTS data) may obtain access to USMS IT systems either through external system connections between the USMS and their agency (see Section B.5), or through individual access after receiving a favorable security approval determination from the Human Resources Division. (See Section F.1, Background Review Prior to Gaining Access to USMS IT Systems.)

5. **External System Connections**: All requests to connect a USMS system to an external system must undergo a thorough review to determine the business need for the connection, the new risks that the external system may bring to MNET and JCON, the new risks that MNET and JCON may bring to the external system, and the mitigating controls that could be implemented to reduce the new risks.

   a. If the external system is hosted by another federal executive agency, at a minimum, the evaluation of the risks will include a review of both agencies' C&A processes, an exchange of accreditation letters between the agencies, and a review of the Security Evaluation Reports for the affected systems.

   b. If the external system is hosted by a government entity at the state or local level, or in the judicial or legislative branch of government, the review of the business need for the connection should include a review of any other federal executive branch agencies already using the external system, with the possibility of finding a link to the system through a federally accredited connection. If there isn't a current federal link to the system, the request for USMS connection should be referred to the DOJ Law Enforcement Information Sharing Program (LEISP) for possible inclusion in their efforts.

   c. In general, a direct connection from USMS to a non-federal executive branch agency or non-government entity will not be permitted; however, each request will be evaluated on a case-by-case basis. Connections will be allowed only after a balanced consideration of the business requirement for the connectivity and the security risks of the connectivity. If connecting the system to the USMS would require a waiver or exception to Department standards, the waiver or exception must be obtained from the Department CIO in accordance with DOJ ITS Standard 1.2, Security Control Review, prior to the connection being established.

   d. Once a favorable review has been completed, the agencies shall sign a Memorandum of Understanding (MOU) outlining the permissions and restrictions placed on the interconnection prior to its implementation. MOUs involving USMS IT interconnections must be signed by the USMS Chief Information Officer (CIO). A listing of all approved IT-related MOUs and a general description of the IT systems covered by the MOUs will be posted on the USMS ITS website so that USMS organizations know what MOUs are in place.

e. Connections between USMS IT equipment and non-USMS IT systems must be documented and approved by ITS. This includes systems generally described as "stand alone" which are not connected to MNET, but are connected to an external system such as a state or local law enforcement agency's server. This also applies to connections between "stand alone" equipment located in another federal, state or local agency that is to be connected to a USMS system, whether or not the USMS system is connected to MNET. The decision to approve or disapprove these connections will be made through the Request for Change (RFC) process (see Section C.3).

6. **System Boundary Analysis:** As part of the annual review of each general support system and major application, the system boundaries of each will be analyzed. Detailed descriptions of the boundaries of each system will be maintained in the System Security Plan for each application. A high level description of the system boundaries will be maintained by the Computer Security Program Manager as a cross reference for all the applications.

7. **Annual Self-Assessments of IT Systems:** As required by NIST and DOJ, the USMS will conduct annual self-assessments of its information systems.

   a. For systems that have already been certified and accredited, the format of the annual self-assessment will depend on the specific requirements from NIST, OMB, or DOJ, but at a minimum will include a review of the questions provided by NIST in Special Publication 800-26. All items identified as needing improvement through the self-assessment process will be documented and a plan of action with milestones will be developed to address the items. The USMS will utilize DOJ-provided standard tools for documenting the items and plans of action.

   b. For new systems that have not been certified and accredited and re-accreditations of expiring C&As, the USMS will utilize the DOJ-provided standard tool for the initial and subsequent annual self-assessments. All items identified as needing improvement through the self-assessment process will be documented and a plan of action with milestones will be developed to address the items.

*Additional References:* For further information, refer to Department of Justice*, ITS Standard 1.2 Security Control Review* (Version 1.0), dated January 30, 2004.

**C. Life Cycle:**

1. **Information Technology Investment Management (ITIM):** The USMS has established an ITIM process to manage the agency's portfolio of IT investments in a way that demonstrates good stewardship, complies with applicable laws and policies, and ensures the effective, efficient, and economical accomplishment of the USMS mission. The ITIM policy is contained in USMS Directive, *Investment Management* and is integrated with a structured system development lifecycle (SDLC) methodology. Both the policy and the accompanying procedures and guidance are posted on the ITS website.

2. **Systems Development Life Cycle (SDLC):** To effectively manage the individual projects included in the USMS IT investment portfolio, the requirements of the DOJ SDLC process were streamlined to produce the USMS SDLC process. The details of the USMS SDLC process are contained in Chapter 5 of the Guide to the USMS ITIM Process.

3. **Request for Change (RFC):** A critical component of the SDLC process is configuration management. No unauthorized or untested software is allowed in the USMS IT environment. The Request for Change (RFC) is used to incorporate independent verification and validation of both a proposal for changes to a USMS system, and the results of any approved changes. This process is contained in the USMS Directive, *IT Security Procedures Policy*, *Appendix 12.7-3 Request for Change*. The RFC process includes the customer's initial proposal for a change, the project manager's initial review of the requirement, a decision to proceed to development, detailed engineering plan, the test plan and results, and a final decision to implement the change. The ITS Program Managers track each RFC and related documents, and issue final approval for the deployment of the RFC after the successful completion of all required steps, including testing.

4. **Configuration Control Board:** As warranted by the substance of a proposed change, the USMS has also established a Configuration Control Board (CCB) to review RFCs as a means of ensuring that the interests of the agency as a whole, and all the IT program areas, are represented in the configuration control decision-making process. The RFC procedures are posted on the ITS website.

*Additional References:* For further information, refer to Department of Justice, *ITS Standard 1.3 Security Planning* (Version 1.0), dated January 30, 2004.

**D. Authorized Processing:** (Certification and Accreditation)

1. Purpose: The purpose of the Certification and Accreditation (C&A) process for all federal government IT systems is to establish uniform procedures for the implementation and protection of those systems. DOJ has issued basic requirements for the implementation of a department-wide C&A program. The USMS participates in this process and ensures that adequate security is incorporated into all phases of the system's life cycle, from planning through developing, deployment, operation, and disposal.

2. Applicability: The C&A process applies to all USMS IT systems and all personnel who use USMS IT systems. The C&A process also applies to any outside organizations, or their representatives, who are granted access to the USMS's IT resources, such as other government agencies.

3. Specific USMS C&A Requirements: The Assistant Director for Information Technology is the USMS designated accrediting authority (DAA), and will make all decisions relating to the operation of the system. The options that the DAA has to choose from include: (1) granting authorization to operate (ATO), (2) issuing interim authority to operate (IATO) under specific terms and conditions, or (3) denying authorization to operate the information system (or if the system is already operational, halting operations) if unacceptable security risks exist. The DAA makes the decision based on the C&A documentation (see Section D.4) and the recommendation of the USMS Computer Security Program Manager (CSPM) who serves as the agency's Certification Official.

   a. Before being placed into production, all USMS systems must receive authority to operate (ATO) through the certification and accreditation process prior to full deployment (except as noted in paragraph D.3.b, below).

      (1) All USMS general support systems and major applications will achieve a separate C&A authority to operate (ATO).

      (2) All USMS minor applications will be certified and accredited to operate through the ATO of an existing USMS IT system (e.g., the Marshals

Network (MNET) or the USMS Justice Consolidated Office Network (JCON)).

(3) Components of a larger system that perform one or more specific functions may be designated as subsystems of the larger system, and will be certified and accredited to operate through the ATO for the larger system. For example, Blackberry Enterprise Exchange Servers are considered a subsystem of the email system, which is part of the JCON general support system, and the Automated Booking Station (ABS) is considered a module or subsystem of the Prisoner Tracking System (PTS).

(4) All USMS classified information technology systems, whether major or minor, will achieve separate ATO status prior to deployment.

b. Full ATO is the goal for every USMS IT system; however, an Interim Authority to Operate (IATO) may be granted under certain circumstances where allowing the system to continue to operate under restrictions is deemed in the best interest of the government. IATO is presumed to be the exception, not the rule, for operating status of USMS systems. The IATO must include planned corrective actions that state how and when existing deficiencies or non-compliance will be mitigated, as well as a scheduled review at the end of the interim period of operation.

(1) An example of a situation in which an IATO may be granted is when a law enforcement emergency presents the need for deploying a new system or a change in an existing system, without adequate time for all security documentation to be completed. In such an instance, all documentation that can be completed should be done, with appropriate notation of the missing information and when it will be developed. In such an emergency, the USMS CCB will work with the USMS security staff to ensure appropriate and timely follow up documents and reviews are provided.

(2) An emergency change to an administrative system may also require a change of status of the system from ATO to IATO. In general, it is expected that emergency changes to administrative systems will be based on law enforcement emergencies or to extremely critical problems identified in an administrative system. An attempt to rush a routine change in either a law enforcement or administrative system because the proposers of the change did not include time for the appropriate C&A reviews will not constitute adequate justification for skipping any part of the C&A review, or for granting IATO status to keep a system operational.

c. Systems under development are expected to deploy a test version of the system in one or more pilot sites prior to beginning full deployment. All C&A documentation should be developed and submitted to review prior to the pilot version of the system being deployed at the first site. Because of the probability that pilot versions will undergo changes before full deployment begins, systems will be granted IATO status for the pilot site(s). The Certification Officer will determine when the documentation has been sufficiently revised so that no other significant changes are expected, and then recommend to the Designated Accrediting Authority to change the system status from IATO to ATO.

4. **Certification and Accreditation Documentation:** Appropriate security documentation will be maintained on every general support system and major application. At a minimum, this will include:

   a. System Security Plan

   b. Risk Assessment

   c. Rules of Behavior

   d. Contingency Plan

   e. Interconnected Data Sharing, Service Level and other Agreements

   f. System Security Test Plan

   g. System Security Test Results

   h. Plans of Action and Milestones for Corrective Actions

   i. Security Evaluation Report

   The agency-wide Rules of Behavior will serve as the basis for each system. If the system owner or system security officer determines that a specific system requires additional rules of behavior not documented in the agency-wide ones, these additional requirements must be documented and all users of that system must acknowledge the system-specific *Rules of Behavior*.

5. **Vulnerability Assessments:** As part of the system security test process, vulnerability assessments shall be conducted on all systems by the computer security team. Systems that may have vulnerability assessments made include, but are not limited to, networks, hosts, applications, routers, switches, firewalls, and databases. The purpose of these assessments is to find threats and vulnerabilities such as: improper access controls; improper access control configurations; weak passwords; lack of integrity of the system software; and not using all relevant software updates and patches. The results of the assessment are documented as part of the security test and evaluation. Identified vulnerabilities will be included in the corrective plan of action for the system.

*Additional References:* For further information, refer to Department of Justice, *ITS Standard 1.4 Processing Authorization (Certification and Accreditation)* (Version 1.0), dated January 30, 2004.

*Additional Information:* on establishing accreditation boundaries for systems, refer to NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal information Systems*, dated May 2004; specifically Section 2.3, Accreditation Boundaries.

**E.** **System Security Plan:** The SSP serves as a significant tool in forming and keeping up-to-date the *USMS Strategic Information Resources Management (IRM) Plan*. Because the USMS Strategic IRM Plan addresses all current IT requirements of the agency, as well as developing requirements, the Strategic IRM Plan should include a summary of the information in each operational systems' SSP. The USMS Strategic IRM Plan and SSPs work in concert to keep each other up-to-date.

*Additional References:* For further information, refer to Department of Justice, *ITS Standard 1.5 System Security Plan* (Version 1.0), dated January 30, 2004.

**F. Personnel Security:** The USMS Human Resources Division (HRD) has primary responsibility for the development and implementation of USMS policy and procedures for personnel security. However, there are a number of aspects of IT security that require interaction with personnel security. This section addresses those specific aspects of personnel security that directly relate to IT security. Within the IT security program, the term "personnel" includes all users of USMS IT systems (as defined by USMS directive, *12.7, IT Security Policy*).

1. **Background Review Prior to Gaining Access to USMS IT Systems:** Prior to receiving access to any USMS IT system, a USMS IT user will have an appropriate background review conducted and successfully adjudicated. The specific procedures for reviewing and adjudicating the backgrounds of USMS IT users are the responsibility of the HRD Office of Background Investigations. Defining the sensitivity level of positions is the responsibility of the HRD. Current definitions are contained in directive, *Security Programs Manager*, *Attachment A - Personnel Security*, Category of Sensitive Positions.

   a. Noncritical-sensitive positions (level 2) include end users who have basic access to USMS IT systems (word processing, email, data retrieval from specific applications, or monitored data entry).

   b. Critical-sensitive positions (level 3) include IT users who have higher levels of access, such as the ability to modify other people's data or to delete records within a system. This level also includes persons who must access systems during operation or maintenance in such a way and with a relatively high risk of causing grave damage, or realizing a personal gain. This level may include privileged users who work in divisions outside of the Office of Information Technology Services (ITS), as well as within ITS. Privileged users are those who have system responsibilities beyond the average user and who are therefore required to understand additional application and environmental functions, as well as security features of the system. Privileged users within the IT staff include, but are not limited to, Systems Administrators, Network Administrators, Firewall Administrators, and Data Base Administrators. Privileged users outside of the IT staff may include persons who have limited application administrator responsibilities.

   c. Special-sensitive positions (level 4) include IT users who design applications or significant features of general support systems, who have the ability to create and delete accounts, or access to systems operations (such as root authority), who support positions that meet the definition of level 4, including the requirement to access national security information (NSI). Standards for determining which positions are categorized as special-sensitive will be set by the USMS Office of Background Investigations with input from ITS.

2. **Periodic Background Reviews:** In addition to the normal periodic reviews of all USMS IT users, persons in special-sensitive positions require Periodic Reinvestigation Single Scope BI (PRIS).

3. **Authorization for System Access:** At the time when a new user is added to a system, or when an existing user's access rights are changed, the user and the user's supervisor must document the level of access that is to be given to the user as part of the new or changed account. Each user will be given the minimal level of access needed to perform their job functions.

   a. New accounts on all USMS general support systems and major applications must be authorized by the user's supervisor before the account is created. Similarly, changes in user access rights to existing accounts on all

USMS general support systems and major applications must be authorized by the user's supervisor before the account is changed. To simplify the process of requesting a new account or changing the access rights on an existing account, the user and the supervisor will complete the *IT User Account Request (UAR) Form, Appendix 12.3A* contained in the USMS directive *12.3, User Access to USMS IT User Systems*. Based on the information provided by the user and the supervisor in the UAR, the user profile will include the applications as listed in the UAR.

b. The basic responsibilities of each user are defined in the Rules of Behavior for each system. No user shall be allowed access to a USMS IT system without first undergoing IT security training and signing USMS *Rules of Behavior, Appendix 12.7-2*, in the USMS directive, *12.7 Information Technology (IT) Security Policy*.

c. Privileged users will be required to sign additional Rules of Behavior for all systems or for specific systems, depending on their range of responsibilities.

d. Prior copies of a user's UAR will be maintained by the computer security team as an external audit trail of changes to a user's profile. It is the responsibility of the System Administrator to forward a copy of the change to the computer security team within three work days of enacting the change.

e. On an annual basis, the list of current users will be reviewed by the application administrator and the data owner. The application administrator will confirm with supervisors that the users are still with the agency, that they still need access to the listed applications, and that the level of access contained in their profiles is still appropriate. It is the responsibility of the application administrator to ensure that supervisors understand the levels of access that are available within the application profiles.

4. **Segregation of Duties:** Within IT systems, there are several levels at which system and application responsibilities need to be separated. Distinct systems support functions shall be performed by different individuals. The support functions of a system shall not be restricted to a single individual. It is the responsibility of the ISSO working with the CSPM to determine the appropriate segregation of duties for IT personnel for each IT general support system or application, and that the specific requirements for each general support system and application are defined within the System Security Plan and related system documentation. The following apply as general rules across all USMS general support systems and applications.

a. End users need to have access to those parts of an application that are relevant to the completion of their job responsibilities, and no more. It is the responsibility of end users to read, understand, and sign the *Rules of Behavior* for all systems that they access.

b. It is the responsibility of the data owner and system owner to work together to determine the practical divisions of information access in order for the mission of the agency to be met.

c. It is the responsibility of the application administrator and the information system security officer (ISSO) to ensure that profiles are established within the application to support the divisions of information access, and that end user accounts are created and maintained based on the correct profile.

d. It is the responsibility of the end users, their supervisors, and the appropriate application administrators to determine the appropriate access level for each user.

e. While application administrators need to have access to extended parts of the application (as compared to end users), they still need to have limits to their access.

f. Application administrator access should not be granted to systems administrators for the platform on which the application runs. At the same time, the systems administrator access should not be granted to application administrators.

g. Within the USMS, the primary responsibility for administering each application shall be assigned to one person known as the application administrator, with a secondary person also designated. Documentation of the individuals filling these responsibilities will be maintained with the application security documents.

h. Within the USMS, the primary responsibility for administering each host server shall be assigned to one person known as the operating systems (OS) administrator, with a secondary person also designated. Documentation of the individuals filling these responsibilities will be maintained with the application security documents.

i. Application and operating system audit logs will be reviewed to ensure that application administrator and OS administrators are not exceeding their designated responsibilities, and that unauthorized changes to systems, applications, or user profiles are not made. The primary review will be by supervisors of application and systems administrators on a weekly basis. In addition, ad hoc reviews of these logs will be conducted by computer security team members. Application administrators, OS administrators, and Systems Administrators are also encouraged to review the logs to ensure that no unauthorized activity is occurring in systems under their responsibility.

5. **Legacy Systems:** Because of the decentralized nature of the USMS work force, the decentralized nature of some of the older major applications, and the limits of the older technology platforms, there are current systems in which the choice has to be made between requiring non-technical staff to perform application and OS administrator level tasks, or allowing technical staff to perform both application and OS administrator tasks. To the extent that no other option is available, technical staff will be authorized to perform both systems and application administration tasks, rather than requiring non-technical staff to perform technical work that they have not been trained to handle, and that takes them away from their normal USMS duties. In these situations, supervisory review of the audit logs should be more frequent (i.e., every second or third day).

6. **Involuntary Terminations:** Special actions must be taken when an "involuntary termination" takes place. Given the potential for adverse consequences, ITS personnel shall do the following:

a. System access should be terminated as quickly as possible. If employees are to be involuntarily terminated, system access should be removed at the same time (or just before) the employees are notified of their dismissal.

b. When an employee notifies an organization of a resignation and it can be reasonably expected that it is on involuntary terms, system access should be immediately terminated.

c. During the "notice of termination" period, it may be necessary to assign the individual to a restricted area and function. This is particularly true for employees capable of changing programs or modifying the system or applications. In some cases, physical removal from the offices may be necessary.

7. **Voluntary Terminations/Transfers:** When a USMS IT user leaves the USMS, the system administrator must initiate action to see that the user's accounts are terminated.. If a USMS IT user changes jobs within the USMS, it is the responsibility of the gaining and losing systems administrators to coordinate the appropriate changes to the user's account, including ensuring that the user's new supervisor completes the UAR designating the new user profile.

8. **Notification of Terminations/Transfers:** Information concerning employee separations will be downloaded from the National Finance Center to a USMS information system, and then will be provided to all systems and application administrators, either through manually-generated notices or automated notices. All systems administrators and application administrators will be responsible for monitoring this information and taking necessary steps to remove or archive user information within their area of responsibility.

*Additional References:* For further information, refer to *Department of Justice, ITS Standard 2.1 Personnel IT Security* (Version 1.0), dated January 30, 2004.

**G. Physical and Environmental Protection:** The Judicial Security Division (JSD), Central Courthouse Management Group (CCMG) has primary responsibility for the development and implementation of USMS policy and procedures for physical and environmental security. However, there are a number of aspects of IT security that require interaction with physical and environmental security. This section addresses those specific aspects of physical and environmental security that directly relate to the protection of all USMS IT systems, including user workstations, as well as USMS computer centers, computer rooms, and telephone (voice and data) circuits and access rooms (also known as telephone closets).

1. **Controlled Physical Access to USMS Office Space**: USMS office space is already controlled access. Therefore, all workstations and computer facilities are housed within controlled access space.

2. **Access Controls for USMS Computer Facilities:** Because USMS office space is already controlled access, most of the specific controls for protecting computer rooms and telephone closets are aimed at tracking physical access to the rooms and materials that may be in the rooms. Based on the size of a USMS office or suboffice, there will be different levels of computer and telephone systems in each location. The following chart shows the major variations that are most likely to exist:

| Office Description | Computer Facility | Telephone Facility |
|---|---|---|
| HQ – Arlington, VA | One Computer Center | Multiple closets |
| Marshals Alternate Computer Center (MACC) | One Backup Computer Center | Single closet |
| Remote HQ locations | One Computer Room | Single closet |
| District Offices | One Computer Room | Multiple or single closet |
| Largest Sub-offices | One Computer Room | Single closet |
| Regular Sub-offices | none | Single closet |

| | | |
|---|---|---|
| Unmanned offices | none | none |

a. USMS access controls can be used to document who had authorized access to specific rooms, and who accessed specific spaces on specific days, but are unlikely to be able to show failed attempts by unauthorized persons to enter a controlled space. Access to computer rooms, data centers, and telephone closets is to be authorized in writing. Visitors to the computer or telephone facilities, including maintenance workers, will be required to sign a log indicating their name, date, time, and purpose of visit. The list of access will be reviewed quarterly by the system administrator and by the district or division security officer to ensure that the people listed continue to need the access.

b. When the rooms have access controls based on card-reader systems, access reports will be reviewed quarterly by the district or division security officer. If a systems administrator is located in the district or division, this function may be delegated to the SA for the computer facilities only.

c. When the rooms have access controls based on punch-key systems, changes to the access codes will be made every 90 days by the district or division security officer. If a systems administrator is located in the district or division, this function may be delegated to the SA for the computer facilities only.

d. When the rooms have access controls based on physical keys, controls of the keys will be maintained by the district or division security officer. If a systems administrator is located in the district or division, this function may be delegated to the SA for the computer facilities only.

3. **Environmental Controls:** ITS works in collaboration with CCMG to establish and implement IT environmental controls standards. The purpose of maintaining these standards is to ensure that servers, network equipment, and telecommunication equipment are maintained not only securely, but also in the most effective environment. To that end, IT system equipment is to be kept in computer and telecommunications rooms. The environmental standards include the following:

a. Space Standards: The recommended standard size of a district computer room is 10' by 10'.

b. Power Standards: Uninterruptible power supplies (UPS) are to be installed on appropriate IT devices. A single UPS to support specific servers and routers or switches is sufficient in all USMS locations other than the HQ and Dallas Computer Centers. Backup generators are installed in these two locations. The minimum power requirements for JCON depend on the number of servers needed at each location. The specific requirements are contained in the *JCON IIA Contingency and Disaster Recovery Plan, Appendix K*.

c. Wiring Standards: The wiring standard for all new wiring is CAT6. Fiber should be added where possible.

d. Fire safety standards: Fire suppression and prevention devices will be deployed in accordance with the resources available in the building, the local ordinances, and requirements for federal buildings. Both computer and telephone facilities will be periodically reviewed to make sure there is no improper storage of ignition sources, including empty or full cardboard boxes.

e. Cooling Standards: USMS computer facilities will have periodic maintenance of the heating and air conditioning systems, performed whenever possible in conjunction with similar maintenance for the building in which the IT facility is located. Separate air cooling systems are required for large or critical computer rooms, especially at for the Headquarters computer room and the MACC. Air conditioned server racks will generally suffice in small to medium computer rooms as an economical yet effective way of providing adequate cooling for IT systems. Specifications for air conditioned racks and larger cooling systems are available on the JCON web site.

f. Supporting Utilities: In cooperation with the physical security programs of the host office, records will be maintained concerning the electrical power distribution, heating plants, water, and sewage for the IT facility. The location of plumbing lines for the building should be maintained by local USMS management and CCMG for use in the event of plumbing or other emergencies in the building or local area.

g. Special Mitigating Factors: In cooperation with the physical security program of the host office, special mitigating factors for possible local disasters (flooding if the building is in a flood zone and on lower floors, earthquakes if the building is in a known earthquake zone) shall be taken into consideration.

4. **Hardware, Software, and Data Loss:**

a. Preventing loss of mobile and portable systems. IT users are responsible for securing their portable and mobile IT systems, and for ensuring the data on these systems is protected.

1) All files on all portable systems must be protected by encryption. Where possible (for example, on all laptop computers), a systems level encryption should be applied. This provides protection for all data on the laptop without necessitating additional actions to be taken by the end users. Where system level encryption is not available, encryption will be applied to individual files. The current approved software and hardware standards for encryption are maintained on the JCON web site.

2) All mobile and portable devices must be protected by passwords.

b. Preventing software license violations/infringements. Only authorized and licensed software may be installed on USMS IT systems. Systems Administrators are responsible for monitoring USMS IT systems within their assigned areas and ensuring that no unauthorized or unlicensed software are installed on them.

c. Preventing interception of data. All users should locate the monitor of their computer work station so that unauthorized persons will not be able to read the monitors. Access to data transmission lines will be limited within all spaces controlled by the USMS. All transmissions leaving USMS-controlled space should have appropriate levels of encryption applied.

d. Reporting loss or theft of USMS IT systems. In the event a USMS IT system or USMS data is lost or stolen, the user will immediately report the facts to the following people:

1) The USMS ITS Helpdesk – which will notify the appropriate system administrator(s) and/or IT security personnel so that appropriate security

measures can be taken (e.g., for mobile or portable IT systems, assistance may be rendered in erasing data or locking encryption keys).

2) The individual's supervisor and/or office property custodian – as required by USMS Property Management regulations for reporting lost and stolen property.

3) The Office of Investigations and/or local law enforcement – as appropriate for stolen property.

*Additional References:* For further information, refer to *Department of Justice, ITS Standard 2.2 Physical and Environmental IT Security* (Version 1.0), dated January 30, 2004.

**H. Production, Input/Output Controls:**

1. **ITS Helpdesk:** The USMS ITS will maintain a Customer Support Helpdesk. The purpose of the ITS Helpdesk is to provide a centralized mechanism for: reporting IT problems; providing Tier 1 assistance; facilitating the assignment of resources to resolve Tier 2, 3, and 4 problems; tracking the status of open calls; and maintaining adequate information to analyze trends from both a technical and a managerial perspective. IT Support Procedures are maintained in *Appendix 12.3B: ITS Support Procedures* of the USMS directive 12.3, *User Access to USMS IT Systems*.

2. **Media Controls:** All forms of media on which electronic copies of USMS data are stored will be marked and protected in a manner commensurate with the level of information maintained on the storage device. The exact methods for controlling and marking the media will be contingent on the type of device, and the technical solutions available at the time the media is in use.

   a. Printed output from USMS IT systems is generally produced within USMS office space. Access to USMS office is controlled and requires that the person have a successfully adjudicated USMS clearance or is escorted at all times. All USMS IT users have clearance to at least the Sensitive But Unclassified level. Therefore, USMS printed information is considered to be maintained in a controlled space commensurate with the level of protection needed for the information. Additional markings are not required unless the printed output is intended for outside distribution.

   b. All sensitive printed media should be destroyed through shredding or "burn bags" when no longer needed.

   c. All electronic media that is no longer usable will have all information removed from its surfaces through degaussing or electronic overwrites. If the media is not to be re-used at all, it will be destroyed.

   d. USMS information categorized at a level higher than SBU has additional handling requirements. The details concerning proper handling of such information is contained in USMS instructions for classified information.

   e. When electronic storage media have to be sent between offices, use of a mailing system that provides an audit trail is required. Logs should be maintained showing that the media has been removed from the first office and arrived at and retained by the destination office. If the media arrives at the destination within the expected time frame, there is no requirement to maintain an audit trail of the tracking information. If the media does not arrive in the expected time frame, or fails to arrive at all, copies of shipping information must be maintained both as a

record of failed service by the mail system and for forensics purposes if theft is suspected.

f. Electronic storage media may be transported between offices by USMS personnel. Logs should be maintained showing that the media has been removed from the first location and retained in the second location. To the extent possible, the information on the media should be protected through encryption while in transit.

*Additional References:* For further information, refer to Department of Justice, *ITS Standard 2.3 Production Input/Output IT Security* (Version 1.0), dated January 30, 2004.

**I. Contingency Planning:** Under the terms of USMS directive, *Space and Facilities*, *Occupant Emergency Program*, it is the responsibility of every USMS organizational component to protect life and property by maintaining an effective Occupant Emergency Plan (OEP) in each USMS building or facility throughout the United States. The following guidance concerns the additional planning needed to maintain or restore IT systems in the event of an emergency.

1. **Continuity of Operations:** While the continuity of operations for all aspects of USMS responsibilities is not wholly dependent on IT functions, IT resources can facilitate all aspects of USMS operations during emergency events. To that end, restoration of IT systems will be a priority in any contingent event. Individual IT contingency plans address the resources necessary to restore operations for each general support system and major application within the USMS. All USMS IT Contingency Plans are on the USMS Intranet. This plan discusses the overall requirements in the event more than one major application and general support system become non-functional at the same time.

a. The USMS Office of Information Technology will operate the Marshals' Alternate Computer Center (MACC) as an active computer center that can become the primary computer center for the Marshals Service in the event the HQ Computer Center becomes inoperable. The MACC is designed to take over all network operations and support major applications that would normally be based in the HQ Computer Center, switching from back-up status to full operations status after an emergency has been declared.

b. IT contingency plans may be used to augment local OEPs to facilitate the continuity of operations that rely on IT systems. Districts/divisions should keep a hard copy of the latest document on hand in the event of a network/system outage. The USMS IT staff will coordinate with senior agency management and program officials to determine the order in which IT systems will be restored in the event of any contingent events that take down more than one system, or to determine the priority order in which different functions will be restored and the levels at which these functions must be maintained if full processing capabilities cannot be restored immediately. General guidance for the decisions that will be made in the event more than one specific IT contingency plan has to be put in effect include:

1) Safety of people (including USMS personnel, employees of the federal courts and other agency, the public, and detainees in custody) will be the highest priority.

2) Restoration of communication services will be the highest IT priority, with voice communication taking precedence over data communication.

3) Restoration of law enforcement applications will be the next highest IT priority, with first attention being given to the Prisoner Tracking System

(PTS) to ensure that each district office is able to locate all in-custody prisoners. Restoration of the Warrant Information Network (WIN) and Automated Prisoner Scheduling System (APSS) will follow.

4) Restoration of administrative and financial applications will follow the law enforcement applications.

2. **Contingency Plan Review/Testing:** All persons with assigned contingency plan responsibilities will be apprised of their responsibilities by the Computer Security Program Manager. The roles and responsibilities will be reviewed and the contingency plan exercised at least once a year by the team of people named within each contingency plan as having critical responsibilities. For USMS applications that involve multiple people performing similar functions in a system restoration (for example, all SAs have the same basic functions within the PTS contingency plan), not all people will be required to participate every year in the contingency plan test. However, the annual test of the contingency plan will include an adequate representation of all possible people with responsibilities, and will rotate among the various people over the course of several years. As part of the annual test, a restoration of the database will be completed using a backup tape.

3. **Backup Capability:** Backups of the operating systems, the application, and the data will be made and maintained in a manner appropriate to the system, and as described in the contingency plan for each system. For example, if an application runs on only one operating system platform, and the USMS has only one of this operating system platform with the only copy of the application running on it, the operating system and application backups need to be made more frequently and more fully than for systems where the USMS has multiple copies of the operating system, the platform, and the application software. In all cases, data needs to be backed up so that work can be restored within a reasonable time, as specified in the system contingency plans. At a minimum, daily backup tapes will be stored in a fire resistant container located outside of the immediate area of the server (it is permitted to be in the same building). At least once every two weeks, additional backup tapes will be shipped to and stored at a location at least 30 miles from the server location, in a fire-resistant container, in accordance with the established ITS site-swapping procedures documented in the application contingency plans.

*Additional References:* For further information, refer to Department of Justice, *ITS Standard 2.4 Contingency Planning* (Version 1.0), dated January 30, 2004

**J. Hardware and System Software Maintenance:**

1. **Hardware Maintenance:**

a. Tiered Maintenance Options: The USMS will maintain equipment through a tiered approach. The tier that best supports each IT system will be decided based on the risk analysis, which includes an evaluation of acceptable “down” time. The tier is then documented in the contingency plan, which relies on the designated approach in the description of required tasks or points of contact for maintenance contracts.

1) Tier 1: Maintaining “hot swap” equipment. The USMS will keep in stock the same type of equipment already configured to support the IT system, so that it can be sent to replace a failing piece of equipment with an expectation of a “plug and play” installation. The time to restore is generally the time required for shipment to reach the destination.

2) Tier 2: Maintaining replacement equipment that can be shipped to replace a failing piece of equipment, but will require on-site installation time.

3) Tier 3: Maintaining hardware maintenance contracts to have contractors replace failing equipment based on a prescribed response time. Note: For equipment that is vital to USMS operations but where maintaining "hot swap" equipment is cost prohibitive, the hardware maintenance contract should provide for 24x7 maintenance with a 4 hour response time. For equipment that is less vital, maintenance may be as low as 8x5 with a next business day response.

b. Preventive Maintenance will be performed on all equipment in accordance with the maintenance contract for the equipment and as recommended by the manufacturer.

2. **Software Maintenance**: For all tiers, software maintenance contracts will be used where it is economically feasible to support the applications in use on the specific equipment. Enterprise licensing agreements will be used to the extent possible to provide the most economical way of obtaining licenses and maintenance contracts.

3. **Persons Authorized to Perform Maintenance:** Only USMS personnel or personnel under contract to the USMS may perform hardware and software maintenance. Contractors must have USMS clearance or be escorted at all times by a person who can be reasonably expected to understand the general work that the contract is performing. Persons who come on-site to perform maintenance functions will be required to sign in and be escorted by USMS personnel with existing clearances.

4. **Sensitive System Utilities:**

a. General Requirements: All operating systems have sensitive system utilities which can circumvent system and application controls. Because of the nature of these utilities, their use must be controlled, monitored, and logged to prevent or detect any misuse of USMS IT resources. All USMS general support systems and major applications will have control mechanisms in place to ensure that access to these utilities are controlled, monitored, and logged to prevent or detect any misuse of USMS IT resources.

b. Authorized Use: Operating system administrators will be the only persons who have access to sensitive system utilities, and only for the equipment that they support on a primary or back-up basis.

c. Temporary Access: Ad hoc access to system utilities may be granted for specific purposes with strict time constraints enforced. The request for temporary access must be made in writing by the person needing the access, and with concurrence by the system ISSO. The written request must define the reasons for the temporary access and the required duration. The decision to grant temporary access will be made by the CIO or designee. Access to the system utilities will be revoked upon completion of the ad hoc task. The security staff will maintain a log of requests for, grants of, and removal of temporary access to system utilities, and will review the status of the access to ensure timely revocation of temporary access.

d. Restrictions: The use of these utilities is not required for the average end-user, and all end-user profiles will ensure that end-user accounts do not access these sensitive system utilities.

e. Monitoring Sensitive System Utility Use: Throughout the year the computer security team will scan all systems to look for unnecessary services or open ports, and for changes to the baseline configuration of the operating system of all servers and databases. Required services and ports will be documented in the C&A documentation for each general support system and major application. Utilities that are not required or not documented as required will be removed from the system.

5. **Virus Detection Software and Training:**

a. Virus detection and elimination software shall be installed on all systems where virus detection software is available, including workstations and servers. Workstations will be configured to receive automated pushes of updates to the virus software and signature files each time the machine is logged onto the network.

b. The computer security team will monitor the release of new virus signature files daily, and update the master files as they are released. To protect against workstation virus contamination, only copyrighted virus detection software that has been licensed and approved through the JCON software Request for Change (RFC) procedures will be installed by ITS personnel on USMS workstations

c. ITS personnel will be trained on the use of the particular virus detection and elimination software that is installed to facilitate the detection and elimination of any virus that infects USMS equipment.

d. End users will be trained to recognize the meaning of messages from the installed anti-virus software, and to report any questions concerning the software or potential viruses to the USMS Helpdesk.

6. **Virus Scans and Reporting:**

a. Every month, ITS personnel will run virus-detection and other security-configuration validation utilities on servers and, on a spot-check basis, on an appropriate sample of workstations. This shall be a full scan of all files. The scan results should be maintained for six months. The scan results will be sent to the Department of Justice in accordance with current reporting standards.

b. Virus scans shall run automatically and record any viruses found. If a virus is found, the user will notify the USMS Helpdesk, who will notify the IT security team in accordance with IT support procedures.

c. Upon notification of a possible virus incident, the IT security team will notify personnel of all interconnected systems to aid in containment and recovery efforts. Using the procedures identified in the *USMS Incident Response Plan*, the Computer Security Program Manager will establish an incident response team who will verify the incident. If the incident escalates to be considered a contingent event, then the respective system contingency plan will be activated. Security and technical personnel responding to the security incident shall coordinate their activities throughout the event.

d. The following automatic virus scans shall be in place:

1) Automatic scan on network log-in;

2) Automatic scan on client/server power on;

3) Specialized mail scans;

4) Automatic scan on insertion of any media;

5) Automatic scan on download from an unprotected source such as the Internet; and

6) Scan for macro viruses.

e. Patch Management: Announcements of new patches to hardware, software, and operating systems will be reviewed for applicability to USMS systems by the IT security working with the JCON Tier 4 Group and appropriate operating system administrators. Applicable patches will be tested as they are available by the JCON Tier 4 Group for all JCON systems and applications, and by the operating systems administrators for non-JCON systems. Patches will be applied promptly after passing all tests. The RFC process shall be utilized to document all configuration changes. All system security parameters shall be checked and verified by the IT security team for proper configuration after applying vendor patches.

*Additional References:* For further information, refer to Department of Justice*, ITS Standard 2.5 Hardware and Software Maintenance* (Version 1.0), dated January 30, 2004.

**K. Data Integrity:**

1. **Reconciliation Routines:** Reconciliation routines such as checksums, hash totals, and record counts will be used by applications (when called for by the sensitivity of the data) to verify data integrity. New applications will incorporate automated means of detecting both intentional and unintentional modifications of data.

2. **Integrity Verification Programs:** Integrity verification programs will be used by applications (when called for by the sensitivity of the data) to look for evidence of data tampering, errors, and omissions.

*Additional References:* For further information, refer to Department of Justice, *ITS Standard 2.6 Data Integrity* (Version 1.0), dated January 30, 2004.

**L. Documentation:**

1. System Administration Manuals: The documentation must be maintained for all hardware and software. For all new systems, and for system undergoing a major modification, vendors shall be contractually obligated to provide the specified documentation prior to placing the system in production. For systems already in use that do not have this level of documentation, reasonable efforts should be made to obtain the missing items.

   a. For commercial-off-the-shelf (COTS) software, copies of vendor-supplied documentation will be maintained sufficient to allow all IT staff who support the system to have access to the documents to enable effective support of the software.

   b. For systems where vendors modify COTS products, documentation of the modifications must be maintained.

c. For government-developed software maintained by USMS IT staff, copies of similar documentation will be developed and maintained.

d. Documentation must be maintained for all hardware. To the extent that initial installation or system set up includes any customization, documentation of the changes must be added to the original vendor documentation.

e. Documentation shall include diagrams of interfaces between systems, network charts, set-up instructions, etc. It should also include emergency and back up procedures, as well as the security documentation required as part of the C&A process.

2. **User Manuals**: This documentation must be maintained for all systems, applications, and software. The manuals should include fundamental concepts and procedures, features/functions, and tutorials important for the operation of the system or application.

3. **Legacy Systems:** IT systems in use prior to the deployment of JCON IIIB (beginning in May 2004) may not have all of the documentation described in this section. If documentation from the initial deployment of the system can be obtained, it should be retained in IT records. If documentation from the initial deployment cannot be found, the configuration of the software and hardware at the time the system was approved to be added to the JCON image will be established as the baseline for the system. All changes to the system from that time forward must be documented through the RFC process (see Section C.3).

*Additional References*: For further information, refer to Department of Justice, *ITS Standard 2.7 Security Documentation* (Version 2.0), dated September 1, 2004.

**M. Security Awareness, Training, and Education:** All personnel who use and/or administer IT systems need to be aware of their role in the protection of the information resources of their agency. This includes both general IT security issues and specific features of the applications and software that personnel access on a routine basis.

1. **Employee Awareness:** An end user needs to understand features such as data input, information retrieval, and protecting printed output. The level of information that a user needs to have depends on the user's role within the IT system.

a. All employees need to be aware of their roles as the first-line users of data. This includes both responsibilities relating to IT security and program area requirements within the application or software. Security awareness will be administered by the USMS IT security program through the use of the DOJ Computer Security Awareness Training (CSAT) program. Program areas are responsible for providing specific application or software training for the users of their systems.

b. It is the responsibility of the USMS IT security program to maintain information on the status of annual refresher training for all USMS users. The USMS IT security program will track this information through the CSAT program tools. If a USMS users is not able to participate in CSAT due to an extended period of time without on-line access to the DOJ training, the USMS IT security team will work with the user's office (district or HQ division) to obtain the appropriate hard copy records and track the user's requirements for annual refresher training.

2. **IT Professional Training:** IT professionals need to understand IT security features such as account profiles, audit logs, and protecting data integrity. Beyond initial awareness of

each application and software system, IT professional need additional training in the functioning of the system.

a. On an annual basis, IT professionals should participate in both technical training and IT security training related to their specific responsibilities. This training may be completed as formal classroom training, on-line course work, or through self-study.

b. Suggested areas of IT security training will be published through the *USMS Security Awareness, Training, and Education (SATE) Plan*. The USMS SATE Plan will follow DOJ recommendations for categories of IT professionals, with additions or deletions to meet the technical requirements of the Marshals Service.

c. It is the responsibility of the USMS IT security program to maintain information on the status of IT professional training related to IT security. The security team will coordinate with the designated ITS training coordinator to maintain this information and to incorporate security training into the overall training requirements for the IT professional staff.

d. In those instances where non-technical employees have to be granted system responsibilities beyond the average user, these privileged users will be required to participate in additional IT security training beyond user awareness course. Non-technical privileged users include, but are not limited to, persons given application administrator responsibilities for a specific office who have limited authority to set up or modify other users' accounts.

3. **IT Security Professional Education:**

a. IT security professionals need to develop expertise in protecting a variety of system platforms and functions. IT security professionals require an even higher level of education in all issues concerning the agency's IT environment. They may be required to develop a level of expertise in the security of applications, hardware, or networks, or to maintain a high level of knowledge in several of these fields.

b. It is the responsibility of the USMS IT security team to maintain information on the status of IT security professional education. The security team will coordinate with the designated ITS training coordinator to maintain this information and to incorporate security education requirements into the overall specialized education requirements for the IT professional staff.

4. **USMS IT SATE Plan:** The USMS Security Awareness, Training and Education (SATE) Program is detailed in the USMS IT SATE Plan. The current version of the SATE plan can be found on the ITS web site on the USMS Intranet.

*Additional References:* For further information, refer to Department of Justice, *ITS Standard 2.8 Security Awareness, Training, and Education* (Version 1.0), dated January 30, 2004.

**N. Incident Response Capability:**

1. **Intrusion Detection Tools:** Network intrusion detection systems (NIDS) is installed on the system in key network segments to identify attempts to penetrate a system and gain unauthorized access. When called for by the sensitivity of the data, host-based intrusion detection systems (HIDS) will be used in addition to NIDS. To aid in intrusion detection, audit trails shall be designed and implemented to record appropriate

information. Intrusion detection logs and audit trails shall be written to a "read only" device either attached to the system or on a secured network interface.

2. **Intrusion Detection Reports:** Intrusion detection reports will be routinely reviewed by the IT security team, and suspected incidents shall be handled according to *USMS Incident Response Plan*. Any intrusion detected shall be reported to the Computer Security Program Manager.

3. **USMS Computer Incident Response Plan (USMS-CIRP):** The USMS recognizes the need to respond to reports of possible IT incidents in an organized and comprehensive manner. The procedures for reporting, responding to, tracking, and closing IT incidents within the USMS are contained in the USMS-CIRP. The current USMS-CIRP is available on the IT web site on the USMS Intranet.

   a. All USMS general support systems and major applications are presumed to be covered by the USMS-CIRP. If a specific system identifies additional requirements for incident responses, the additional requirements will be reviewed by the IT security team to see if they should apply to all USMS systems. If they should be applied to all systems, the USMS-CIRP will be modified by the IT security team to reflect the new requirements. If the additional requirements apply only to one system, the Contingency Plan for that system will be annotated by the system's ISSO to include the additional requirements.

   b. All USMS IT systems users are responsible for being aware of possible incidents on USMS IT systems. If an incident is suspected, users will report the problem to the USMS Helpdesk, which will follow the procedures in the USMS-CIRP.

   c. The Helpdesk will implement the USMS-CIRP plan to determine if the suspected activity is an incident. If the suspected activity is deemed to not be an incident, the Helpdesk will assist the user in solving whatever technical problems are happening. If the suspected activity is deemed to be an incident, the USMS-CIRP will proceed and the Help Desk will notify the CSPM or a CSPM designee. The CSPM will create the CIRP Team to address the specific incident and designate a person to lead the response. The CIRP Team will investigate the incident and determine the appropriate actions to resolve the incident. The CIRP lead person will report the status to the CSPM. The CSPM will, in turn, report to DOJCERT and those who have a legitimate need to know about the incident. If the incident escalates and is considered a contingent event, then the CSPM will notify the appropriate system contingency team.

4. **DOJCERT Reporting:** All confirmed IT incidents are reported to DOJCERT by the CSPM. Additional reports, such as to FedCIRP, NIPC, or local law enforcement authorities are coordinated through DOJCERT, if necessary, by the CSPM.

5. **Reporting Problems that Are Not Incidents:** All USMS IT systems users are responsible for also being aware of events which do not meet the definition of incidents but which can cause problems on USMS IT systems. The most obvious example of this level of problem is email SPAM. Although SPAM might be the initial sign of a denial of service attack on the network or the first symptom of a virus threat, most often it is simply unsolicited and unwanted email. USMS users should report all SPAM to the USMS Reports email account, where it will be reviewed to confirm that it is not part of a denial of service or virus attack. The volume of plain SPAM received in the USMS will be reported to DOJCERT on a monthly basis.

*Additional References:* For further information, refer to Department of Justice, *ITS Standard 2.9 Incident Response and Reporting* (Version 1.0), dated January 30, 2004.

**O. Identification and Authentication:** All USMS IT systems are required to incorporate both user identification (userid) and user authentication (passwords). The combination of userid and password must be unique for each user. Each user is required to have a unique userid logon.

1. **Password Policy Compliance:**

a. Minimum requirements and standard conventions for passwords are established by the Department of Justice; however, USMS users are encouraged to use the strongest possible passwords in each system. The *Rules of Behavior, Appendix 12.7-2*, in the USMS directive, *12.7 Information Technology (IT) Security Policy*, Paragraph D.2, explain the general characteristics of a strong password, including a minimum of 8 characters; a combination of letters, numbers, and symbols; and being hard to guess (i.e., not your spouse's name or your favorite sports team).

b. Passwords are required to have configuration requirements, including:

1) maximum duration – 90 days;

2) minimum length – 8 characters;

3) composition – combination of letters, numbers, special characters;

4) inactivity locks – after 20 minutes of no use; and

5) recycling limits – cannot repeat for 6 cycles.

c. Initial and replacement passwords must comply with the password characteristics, and must be distributed in a secure manner. The order of preference for distributing the initial password is direct contact between administrator and user, through email account to the specific user, by sealed envelop. Distribution over the telephone is authorized only where the identify of the user can be confirmed.

d. Each IT system must implement compliance with password policies. Applications that rely on default features in operating systems or software must ensure that the defaults comply with the password policies or can be changed to do so. Access scripts that contain embedded passwords are prohibited. Where this feature cannot be permanently turned off (as is the case in certain Microsoft dial-up login scripts), users must be instructed not to save their passwords in the scripts.

e. All passwords will be considered highly sensitive are NOT to be shared with anyone. If it is necessary to reveal individual passwords to ITS staff for diagnostic reasons, the respective passwords shall be changed immediately thereafter by the user.

f. Passwords shall be controlled by the user and safeguarded (e.g., not be affixed to any surface of computer or telecommunications systems) so that no other person shall gain knowledge of the user's password. Each user will be held accountable for all actions performed on the user's account.

2. **Generic Accounts:**

   a. System defined generic accounts that allow non-unique account names (such as guest, anonymous and other optional generic names) are prohibited and shall be removed and disabled. Temporary use of generic accounts for training purposes (such as Train1, Train2, etc.) will be allowed for the length of time needed to complete the training for a specific system. These temporary accounts will have the minimum possible user profile, providing access only as needed for the class.

   b. Mandatory (operating system) generic accounts such as 'root' or 'administrator' must be accessed from a current valid logon that provides an audit path with explicit user identity. Privileged users who have access to these mandatory generic accounts must be designated in writing in the system security plan. Such designations will be kept to a minimum, limited to the designated primary and backup systems operators to the extent possible. In applications where direct login to mandatory generic accounts is necessary, this access will be restricted to the system local console and will be physically secured. These requirements do not apply to service accounts required by some applications; however, these service accounts should be appropriately documented in the administrator manuals for the impacted systems.

   c. Accounts which are identified by a unique name (such as a district or division office) are allowed. These accounts must be assigned to one person as the account owner. The account owner may assign "proxy rights" to other users as appropriate (for example, within an email account). The account owner is ultimately accountable for all activity generated by this account.

   d. Reviews of designated non-technical users with privileged access will be conducted annually by the IT security team working with the ISSO for each system, to verify that the privileged access is still needed.

3. **USMS Password Database:** The root level passwords for the applications and servers will be maintained in the USMS password database system. Other IT system administration passwords, including for routers and switches, must also be maintained in the USMS password database. IT personnel are responsible for changing their assigned passwords every 90 days, or whenever a possible breach in the password has occurred. Reports will be generated at the end of each quarter to ensure that the passwords for all devices stored in the password database system have been changed in accordance with the required time frames. The IT security staff is responsible for the oversight of this database.

4. **Vendor-Supplied Passwords:** All vendor default passwords must be changed as soon as the piece of hardware or software is brought on-line within the USMS systems. All replacement passwords must meet USMS password standards for length, characteristics, retention, etc.

5. **Temporary Password**s: If a USMS collaterally assigned employee, vendor, or third-party contractor needs to log into a device (such as a router) to provide maintenance or diagnostic services, a temporary password for that device will be set up. As soon as the maintenance or diagnostic services have finished, the temporary password must be replaced with a new permanent password that meets all USMS password standards.

6. **Message Authentication:** Message authentication is an integral element of the Public Key Infrastructure (PKI) implementation. Systems which utilize message authentication technology shall use that technology in place of written signatures on electronic documents. The USMS is participating in the DOJ PKI program, and will implement the

requirements of that program as they are defined. Refer to the Department Public Key Infrastructure Standard (in development) for additional information.

*Additional References:* For further information, refer to Department of Justice, *ITS Standard 3.1 Identification and Authentication* (Version 1.0), dated December 4, 2003.

**P. Logical Access Controls:**

1. **Account Locking:**

a. Workstations must lock after 20 minutes of inactivity from either a keyboard or mouse. The desktop lock provided by the operating system in Windows XP (or compatible level) is sufficient.

b. Accounts which have no activity for more than 30 days will be made inactive but will not be deleted. Due to the nature of various USMS positions, it is possible for current employees to be detailed to different task forces and job functions for periods of 90 days or more. Therefore, accounts will not automatically be deleted based on inactivity. After one year of inactivity, the application administrator will request a review of the account by the user's supervisor. Unless the user's supervisor provides justification to the Assistant Director for Information Technology for maintaining the account (i.e., because the user is on military leave but still expected to return to work), the account will be deleted at that point..

c. Because administrator accounts provide access to systems to perform support services may not be used as frequently as general user accounts, but must be active when the support services are needed, the administrator accounts are not subject to being made inactive solely on the basis of lack of activity. The DOJ standard of 90 day review for account inactivity will be used for the administrator accounts, as established in DOJ IT Security Standard *Access Controls* Version 2.0. If the administrator account is not used within 90 days, the systems administrator will be asked to confirm the continued need for the account. The system administrator's supervisor will review the appropriate systems logs to verify that the account has not been compromised. If the systems administrator cannot confirm the continued need for the account, it will be disabled immediately.

2. **Remote Access:**

a. Remote access to USMS IT systems is provided by the Justice Secure Remote Access (JSRA). Remote Access is defined as end user device access to USMS IT Systems. No other forms of remote access are allowed.

b. In emergency situations, remote access to USMS IT systems may be provided on a temporary basis via the USMS Secure Virtual Private Network (SVPN). An approved RFC is required to implement SVPN access during a contingent event.

c. Devices connected to MNET may not have any other active network connection. This includes all network connections including ethernet, telephone modems, cable modems, DSL, any wireless connection, etc.

3. **External Communication from USMS Network (Firewalls):** External Communication from USMS Network (Firewalls): All communication with external networks must traverse through the USMS firewall. The USMS firewall will maintain a minimum configuration

setting in line with the DOJ standard for firewalls and detailed in the network configuration documents. Guest and anonymous accounts are not authorized in the network.

4. **Internal Communication within USMS Network (Routers, etc.):** All communications within the USMS IT environment will be controlled through the use of standard network equipment, including routers, switches, and hubs. Baseline configurations for each category of equipment will be maintained in the network configuration documents.

5. **Wireless Access (WiFi) within USMS Information Technology (IT) Systems:** This section describes the authorized use of wireless access (Wi-Fi) systems and the corresponding compliance enforcement procedures.

   a. Authorized Use of Wi-Fi Systems in USMS:

      1) Network Usage: Wi-Fi technology is NOT authorized for use within the USMS Network (MNET). No wireless access points or wireless adapters may be connected to USMS IT equipment that is also directly connected to the USMS network (MNET).

      2) Mobile Usage: Personnel outside of USMS office space may use commercially available Wi-Fi hotspots in conjunction with a USMS laptop and Justice Secure Remote Access (JSRA) token to remotely access the USMS network. Wi-Fi cards must be approved for use on USMS systems. Wi-Fi cards may not act as an access point, or in "ad-hoc" mode. Users must initiate a JSRA session immediately upon connection to the wireless network to encrypt and secure communications.

      3) Exceptions: Any exceptions or waivers to this policy must be granted by the Assistant Director for Information Technology (CIO). Exceptions may be granted on a temporary basis in exigent or contingency circumstances.

   b. Detection and Removal of Unauthorized Wi-Fi Systems: USMS ITS staff will detect and deactivate or remove Wi-Fi equipment that is connected to the USMS network or USMS information technology systems.

   c. Detection and corrective action procedures

      1) In conformance with USMS and DOJ procedures, ITS security staff will conduct monthly scans throughout the USMS network to identify wireless access points.

      2) Additionally, ITS personnel will perform spectrum scans at USMS offices on an ad-hoc basis. ITS will utilize wireless scanning devices to detect signals compliant with the 802.11a, 802.11b, 802.11g and pre 802.11n standards in the 2.4 GHz and 5.2 GHz ranges.

      3) Upon detection of a wireless signal in USMS offices, ITS personnel will locate the source, determine if this signal is associated with USMS IT systems, and, if necessary, disconnect the equipment from the USMS network and report the incident to the USMS Computer Systems Security Officer (CSSO)..

*Additional References:* For further information, refer to Department of Justice, *ITS Standard Logical Access Control* (Version 2.1), dated March 2007.

## Q. Audit Trails:

1. **Minimum Standards for Operating System Audit Logs** (under development)

| ***Logs must be able to address:*** | |
|---|---|
| Time Stamping<br>Access Control for On-line Audit Logs<br>Separation of Duties for Security Personnel<br>Review of Audit Records using utomated Tools<br>Keystroke Monitoring | After-the-fact Investigations<br>Storage/Access Control of Off-line Audit Logs<br>Review Frequency of Audit Trails<br>Investigation of Suspicious Activity |

2. **Minimum Standards for Application Audit Logs** (under development)

| ***Logs must be able to address:*** | |
|---|---|
| Time Stamping<br>Access Control for On-line Audit Logs<br>Separation of Duties for Security Personnel<br>Review of Audit Records using Automated Tools<br>Keystroke Monitoring | After-the-fact Investigations<br>Storage/Access Control of Off-line Audit Logs<br>Review Frequency of Audit Trails<br>Investigation of Suspicious Activity |

3. **Remote Logging for Operating Systems and Applications:** As an additional precaution against accidental or intention tampering with audit logs, and to ensure that logs are maintained for an appropriate length of time, both system audit logs and application audit logs will be automatically copied to a remote log server (syslog). Access to the syslog server will be limited to the number of people needed to effectively conduct the review of the logs.

4. **Review of Logs:** System and application logs shall be reviewed by the designated technical teams, by supervisors of the administrators supporting the system (applications, operating systems, or SAs), or by the security team. Because administrators with root-level access to the operating system or application may have access to logs by default, they cannot be the only persons responsible for reviewing the logs, and cannot be the person responsible for reviewing the syslog version of logs from their own system or application.

5. **Frequency of Reviews:** will be commensurate with the criticality of the systems.

   a. Firewall logs will be sent daily to a remote log server (syslog), and will be reviewed daily by IT security staff.

   b. Core routers logs will be sent daily to a remote log server (syslog), and will be reviewed daily by network security staff.

   c. District office router logs will be sent daily to a remote log server (syslog), and will be reviewed daily by network security staff.

   d. Suboffice router logs will be sent daily to a remote log server (syslog), and will be reviewed weekly by network security staff.

   e. Exchange server logs will be sent daily to a remote log server (syslog), and will be reviewed weekly by JCON Tier 4 security staff.

f. Major applications server system logs will be sent daily to a remote log server (syslog), and will be reviewed monthly by the supervisors of the operating system administrators.

g. Major application logs will be sent daily to a remote log server, and will be reviewed monthly by the supervisors of the application administrators.

*Additional References:* For further information, refer to Department of Justice, *ITS Standard 3.3 Accountability and Audit* (Version 1.0), dated December 4, 2003.

| **By Order of:** | **Effective Date:** |
| --- | --- |
| /S/<br>Chris Dudley<br>Chief of Staff<br>U.S. Marshals Service | March 26, 2008 |

## 12.7.2 RULES OF BEHAVIOR

**A. Introduction:** The United States Marshals Service (USMS) Sensitive But Unclassified (SBU) Computer and Telecommunications Systems Rules of Behavior document is intended to establish ethical and practical standards in support of the USMS Directives and the USMS security training and awareness program. It was prepared to meet the requirements of OMB Circular A-130, Department of Justice (DOJ) Order 2640.2E and the DOJ Information Technology Security Program Operating Manual (ITSPOM). All users are expected to become familiar with DOJ Order 2640.2E and abide by the instructions contained in this document. Any questions concerning the applicability or interpretation of any of these rules of behavior should be directed to ITS.

**B. Applicability:** These rules are applicable to all individuals (whether they be end-users, administrators, etc.) utilizing USMS SBU computer or telecommunications systems. All SBU computer and telecommunications system users are responsible for reading and complying with the rules of behavior, and any appendices issued for specific systems, and signing the appropriate acknowledgment form prior to operating USMS SBU IS resources.

Failure to sign the Rules of Behavior and return it to the appropriate supervisor may result in the denial of access to USMS computer and telecommunications systems. Failure to comply with the rules of behavior is a security violation and may result in disciplinary action.

**C. General Principles:** Because written guidance cannot cover every contingency, personnel are asked to go beyond the stated rules, using their best judgment and highest ethical standards to guide their actions. Personnel must understand that these rules are based on Federal laws, regulations, and DOJ Orders. As such, there are consequences for non-compliance with rules of behavior. Depending on the severity of the violation, at the discretion of management and through due process of the law, consequences can include: suspension of access privileges, reprimand, suspension, demotion, removal, and criminal and civil penalties.

1. **Accountability:** Employees are responsible and will be held accountable for their actions related to USMS information resources entrusted to them.

2. **Confidentiality**: Employees must protect all USMS documents and data that contain SBU information from disclosure to unauthorized individuals or groups. Employees must understand that they will acquire and use sensitive information only in accordance with established policies and procedures. This includes: properly destroying sensitive information contained in hardcopy or softcopy; ensuring that sensitive information is accurate, timely complete, and relevant for the purpose which it is collected, provided, and used.

3. **Passwords and User Identification (user ID)**: Employees must protect information security through effective use of user IDs and passwords. Each system user will be assigned a unique personal identifier and password (minimum length is eight alphanumeric characters) to establish all personal accounts and access privileges for the individual. The initial password will be changed immediately upon first use of the account.

4. **Hardware/Software**: Employees must protect computer equipment against waste, loss, damage, abuse, misappropriation, and unauthorized use. This includes USMS-owned resources located at employees place of residence and portable personal computers used for business while on travel. Employees will comply with all copyright licenses associated with the USMS networks. Employees will comply with the personal use of government equipment in accordance with USMS policies and procedures.

5. **Reporting:** Employees must report security violations and vulnerabilities to the proper authorities.

6. **Privileged Users:** Privileged users must perform their duties meticulously and reliably in order to preserve information security. Privileged users include: system administrators; computer operators; system engineers; those with control of the operating system; network administrators; those who have access to change control parameters for equipment and software; data base administrators; those who control user passwords and access levels; and system maintenance personnel.

7. **Remote and Work-at-Home Users:** Remote and work-at-home users must protect hardware, software, and information to the USMS security specifications including procedures for destruction of hard copy material(s). Users shall have access only to those resources required for the position they hold and have authority to use, as established and defined through an agreement with the supervisor. Security responsibilities must be explicitly stated in such agreements. Other requirements for remote and work-at-home personnel include: using software according to licensing agreements; ensuring that confidentially-sensitive information that is downloaded is secure, and that dial-in access is secure; and being alert for anomalies and vulnerabilities, reporting these to proper officials, and seeking advice when necessary.

   When working at home, employees must establish security standards at the alternate workplace sufficient to protect hardware, software, and information. This includes having only those resources needed and having authority to use; establishing a thorough understanding and agreement with their supervisor as to what their security responsibilities are; using software according to licensing agreements; ensuring that confidentially-sensitive information that is downloaded is secure; being alert for anomalies and vulnerabilities; and reporting these anomalies to proper officials and seeking advice when necessary.

   The USMS will regularly review telecommunications logs and DOJ phone records, and conduct spot-checks to determine if users are complying with controls placed on the use of dial-in lines. Only DOJ-authorized USMS Internet connections will be allowed, and all connections must conform to DOJ's USMS security and communications architecture.

8. **Users of Personal Information:** Users must acquire and use personal information only in ways that respect an individual's privacy. This includes: properly destroying personal information contained in hard copy or soft-copy; ensuring that personal information is accurate, timely, complete, and relevant for the purpose which it is collected, provided, and used.

**D.** **System Access and Use:** Before granting access to computer and telecommunications systems, system administrators will determine personnel access needs based upon written requests for access to systems and applications provided in writing by the first line or higher supervisor of the person or persons for whom access is requested. This request will be in the form of a signed memorandum request containing the information described in the *Appendix 12.3A: IT User Account Request (UAR) Form* contained USMS directive *12.3 User Access to*

*USMS IT User Systems*. All USMS system administrators for the systems and applications for which they are responsible will maintain a permanent record of all such requests.

Any changes to be made to a user's access privileges shall use the same formal request format as the original access request. Changes to access privileges include adding access membership in a shared directory, or adding access to additional applications or resources in another domain (not their home domain), etc.

Supervisors are required to notify the administrator when the account is no longer necessary.

1. **Information Security:**

All data processed, stored or transmitted on USMS computer or telecommunications system resources shall be protected, at a minimum, at the level for which the computer or telecommunications system is accredited until it is reviewed and determined to be of lesser sensitivity.

Classified national security information or Grand Jury information shall only be processed on computer or telecommunications system equipment accredited for the processing of classified national security information.

DOJ Order 2620.7, Limited Official Use delineates which information shall be protected as Limited Official Use (LOU) information. LOU information may be processed on USMS computer and telecommunications systems. All USMS IS output that contains LOU information shall be appropriately marked or labeled and stored by the user who generated the material in accordance with the provisions the DOJ Order 2620.7.

Diskettes or other media containing sensitive information shall be appropriately labeled and stored in approved locked containers (e.g., desks, filing cabinets, etc.) USMS LOU information (files) stored on magnetic media shall be overwritten by approved overwrite procedures or degaussed prior to release of the storage media outside the USMS. Users should not store data on diskettes using a workstation's A: drive, unless it is necessary and such storage of data has been specifically authorized. Any diskette that contains USMS LOU information or classified information shall be appropriately marked and safeguarded.

Users shall ensure that unauthorized personnel cannot view any data that is visible on the workstation monitor screen. Users shall log off their workstations whenever they are away from the immediate work area, unless an approved screen saver feature with a password enabled is properly invoked. An approved screen saver feature may be used to protect LOU data when the workstation is left unattended for short periods, and the user will remain in the immediate area (e.g., retrieving output from the printer, visiting the restroom). If a user is going to another floor or leaving the building, the user shall log off their workstation before leaving the area. Only the approved screen savers installed by system administrators are authorized. No other screen savers may be installed.

2. **Passwords:**

a. Passwords shall be a minimum of eight characters in length.

b. It should be something you can easily remember, but should not be something that another can guess, so do not use the name of your spouse, pets, or children.

c. Passwords shall not be shared or written down.

d. Do not accept another user's password even if offered.

e. Passwords will be changed at a maximum interval of 90 days, or less if required by specific system policy.

f. Users will be locked out of the system after three consecutive incorrect password entries.

g. Passwords are case sensitive. Users should not attempt to enter a password with the "caps lock" key enabled.

h. When the screen saver is authorized for use, a user's screen saver password should have the same characteristics as the password used to log-on to the system, but shall be different from the system password.

i. System administrators or other system support personnel have no way to look up your password. If you forget it, your system administrator or other system support personnel will change it and make you pick a new password.

j. A new password cannot be the same as one you used recently.

k. If there is a reason, you may change your password before the end of the system prescribed maximum interval, but only after three days have elapsed since the password to be changed was created. If there is a compelling reason to change the existing password before the end of the three-day period (such as a suspected compromise) contact the system administrator or other system support personnel.

3. **Electronic Mail Use:**

Government-provided electronic mail is intended for official and authorized purposes. Electronic mail users must exercise common sense, good judgment, and propriety in the use of Government resources. The presumption is that no notice except those sent by system administrators or support personnel is so important that it should be broadcast globally to large personal groups or to everyone within an organization or USMS-wide without the approval of the appropriate office head. In this issuance broadcast messages are messages sent to public groups listed in the system's address book or large personal groups.

In accordance with 28 CFR 45.4 “Personal Use of Government Property,” employees are specifically prohibited from using USMS/DOJ electronic mail systems to distribute information on any non-Government activity, including (but not limited to) charitable events, religious observances, fund-raisers, and personal business. Employees who misuse Government resources in this way may have electronic mail privileges withdrawn and may be subject to disciplinary action.

Government employees should have no expectation of privacy when using electronic mail systems. Electronic mail is not confidential. System administrators and others with special system-level access privileges are expressly prohibited from reading the electronic mail of others unless authorized by appropriate senior management officials. However, users should understand there is no guarantee that technical or administrative problems may not create a situation in which it is necessary for an administrator or system manager to read message text. Moreover, USMS views electronic mail messages to be Government property, and officials may have access to those messages whenever there is a legitimate Government purpose for such access. Users should treat the electronic mail system like the use of a Government-provided interoffice mail system.

4. **Responsibility and Accountability on USMS Information Systems**: All computer and telecommunications users will be held strictly accountable for their actions while on the USMS system. These rules of behavior apply even if you do not take time to read them. Violation of these rules may result in disciplinary action. User activity is continuously monitored and system activity is audited to detect unauthorized activity or suspicious behavior. Unauthorized activity or suspicious behavior by users may result in loss of access, written reprimands, loss of job, fines, or imprisonment under the provisions of the USMS personnel policies and applicable statutes.

5. **Specific DOs and DON'Ts:**

a. **Dos:**

DO take necessary actions to ensure that only authorized personnel use your computer and telecommunications systems.

DO safeguard computer and telecommunications resources against waste, loss, abuse, unauthorized use, and misappropriation.

DO protect equipment (workstation, diskettes, etc.) to ensure that it is clean and protected from anything that may cause damage. This includes taking precautions to ensure that food, drinks, and other hazards do not damage workstations or media. Also, keep storage media away from devices that produce magnetic fields.

DO report all security incidents or suspected security incidents, including virus infections, to ITS. (Note: The term "security incident" includes any event that may result in the disclosure of sensitive or classified information to unauthorized individuals or that results in unauthorized access, modification, or destruction of system data, loss of system processing capability, or loss or theft of any computer system media.) Report any actual or suspected security vulnerabilities to your first line supervisor and/or to ITS.

DO take action to reduce damage caused by security incidents, as appropriate (e.g., lock up property, log-off of the computer, disconnect a workstation with a virus from the LAN)

DO comply with copyright and site licenses of proprietary software. No personally purchased software or public domain software is allowed on USMS computer or telecommunications system without prior written permission of ITS. DO make backups of data and files stored on PCs or workstations on a regular basis.

DO use only the computer and telecommunications resources for which you have been granted authorization to access.

b. **DON'Ts:**

DON'T remove any computer or telecommunications resource from USMS premises without an official property pass and written approval from your supervisor. Resources may only be removed from USMS premises for official use.

DON'T install any software on your workstation or any other computer or telecommunications resources. Only your system administrator (or their

designated representative) is authorized to load software on the servers or workstations.

DON'T install modems (either internal or external) to your workstations, servers or any other computer or telecommunications resource.

DON'T add any additional hardware or peripheral devices to your workstations, servers or any other computer or telecommunications resource. This includes all devices such as extra memory, hard drives, printers, scanners, additional servers, additional processors, etc. Only the ITS system administrator can direct the installation of hardware on USMS IS. Also, don't reconfigure any IS hardware or software.

DON'T transmit LOU or other sensitive information across public access systems.

DON'T distribute or receive documents via public access systems in violation of copyright laws.

DON'T access external computer systems (such as bulletin boards) unless necessary to perform an official duty.

DON'T attempt to gain access to information to which you do not have authority.

DON'T continue use of any PC, LAN system, or software that shows indications of being infected with a virus.

DON'T retrieve information for someone who does not have authority to access that information.

DON'T store combustible materials near a computer or telecommunications system.

DON'T allow someone to perform maintenance without proper identification.

DON'T eat, drink, or smoke near computer or telecommunications resources

United States Marshals Service POLICY DIRECTIVES

**INFORMATION RESOURCES MANAGEMENT**

**12.7.3 Request for Change (RFC)**

**Overview** | **The RFC Process** | **Appendix A: Flow Chart** | **Appendix B: RFC Categories**
**Appendix C: Concept Proposal Form**

**Date:** **July 27, 2009**

**Contacts:** Lisa Davis, Chief Information Officer; Gwen Miller, Chief Technology Officer

**Update of:** **Appendix 12.7-3, REQUEST FOR CHANGE (RFC) PM-2007-1 – Dated June 13, 2007**

**Purpose:** The System Change Request Procedures provide a structured process for proposed changes to the Marshals Service Information Technology (IT) systems and resources. The RFC Flowchart and narrative is intended to formalize and clarify the process and flow of a change request.

**Audience:** The RFC process is intended for use by all USMS Personnel.

**Reference:** The RFC process is a subset of the USMS IT Configuration Management Plan. The purpose of the United States Marshals Service (USMS) Configuration Management Plan (CMP) is to describe the key Configuration Management (CM) activities and practices for the development and operation for all Information Technology (IT) systems throughout the USMS System Development Life Cycle (SDLC). Web Version | PDF Version

**Acronyms** The following table contains a list of acronyms used in the RFC process.

| Acronym | Definition |
|---|---|
| AM | Account Manager |
| C&A | Certification and Accreditation |
| CCB | Configuration Control Board |
| CDR | Critical Design Review |
| CM | Configuration Management |
| CI | Configuration Item |
| CIO | Chief Information Officer |
| CMP | Configuration Management Plan |
| CISO | Chief, Information Security Officer |
| COTS | Commercial Off The Shelf |
| CTO | Chief, Technology Officer |

| | |
|---|---|
| D/CIO | Deputy, Chief Information Officer |
| DAA | Designated Approving Authority |
| ERB | Engineering Review Board |
| FCB | Functional Control Board |
| FRD | Functional Requirements Document |
| GOTS | Government Off The Shelf |
| IPT | Integrated Product Team |
| ISSO | Information System Security Officer |
| IT | Information Technology |
| ITD | Information Technology Division |
| NIST | National Institute of Standards and Technology |
| PDR | Preliminary Design Review |
| PM | Program/Project Manager |
| RFC | Request For Change |
| SDLC | System Development Life Cycle |
| SP | Solution Provider |
| SRR | Systems Requirements Review |
| USMS | United States Marshals Service |
| VPR | Vulnerability Patch Requirement |

**Roles and Responsibilities:** The recommended roles and responsibilities are defined below ***Error! Reference source not found.***.

| Roles | Responsibilities |
|---|---|
| **USMS D/CIO** | • Chair FCB<br>• Make implementation assignment for RFCs<br>• Provide approval or denial within the FCB<br>• Provide advice and consultation to ERB to ensure effective configuration management process<br>• Assign RFC to appropriate individual |
| **USMS CTO** | • Chair of the ERB<br>• Performs engineering assessment of RFC Design for compliance with USMS architecture<br>• Provide approval or denial within the ERB<br>• Provide advice and consultation to CCB to ensure effective configuration management process |

| | |
|---|---|
| **USMS CISO** | • USMS Configuration Manager<br>• Chair of the CCB meetings<br>• Approve disposition of each RFC<br>• Manage escalation process when a RFC is referred for higher-level approval or input<br>• Ensure action is taken on RFC in a timely fashion |
| **Executive Secretariat** | • Prepares, coordinates, and distributes the FCB/ERB/CCB meeting agendas<br>• Act as recording secretary during FCB/ERB/CCB meetings<br>• Prepare and distribute the FCB/ERB/CCB meeting minutes<br>• Prepare the written synopsis of matters considered and recommendations made by the FCB/ERB/CCB<br>• Distribute copies of synopsis to FCB/ERB/CCB members after FCB/ERB/CCB chair approval<br>• Maintains all documentation collected for all FCB/ERB/CCB |
| **Security Representative** | • Review and evaluate changes to ensure the integrity of the system<br>• Ensure mitigation of security risks<br>• Review RFC to ensure that the modified configuration maintains its certification and accreditation status<br>• Review and evaluate changes to ensure that the proposed changes are in accordance with DOJ and USMS security policy and guidance as well as applicable federal laws, directives, policies, regulations, standards, and guidance<br>• Advise appropriate security organizations on security status of configuration changes<br>• Sign the final CCB approval acknowledging that the change has been reviewed relative to security issues |
| **USMS FCB Integrated Product Team (IPT) Members** | Maintain expertise in processes and best practices<br>Review, evaluate, and coordinate proposed changes submitted for consideration with other stakeholders, as appropriate, to determine impact of all proposed changes<br>Attend meetings to present position statement on proposed changes<br>Assist in the preparation of concept proposal/functional requirements document<br>Assist in determining the impact of proposed changes as a subject matter expert where appropriate<br>Perform other tasks as assigned by the Board Chairs |

| | |
|---|---|
| **PM/AM/SP** | • Generate Concept Proposal with input from user<br>• Provide oversight of CM activities to ensure successful program performance and compliance with program policies and federal regulations<br>Ensure adequate resources are available for CM activities<br>Ensure that support team leads and other persons in management or supervisory roles support the objectives of the CMP<br>Review CM metrics and other reports<br>Ensure the execution of appropriate system testing prior to releasing versions<br>Publish final system test results to CCB members and other stakeholders<br>Periodically provide updates to customer on the RFC progress |

**RFC Process: Overview**

The following steps outline the RFC process. In addition, a flowchart is also provided that outlines all contingencies in the decision making process.

Purchase approvals DO NOT preclude the need to file an RFC. Examples of purchases that do require an RFC are new servers, network devices, or unapproved software. Examples of purchase that do not require an RFC are additional licenses for approved software. The RFC must be submitted and approved PRIOR to the purchase.

*Attachment A* contains the flowchart associated with the RFC process. The flowchart and associated narrative serve as "standard operating procedures."

*Attachment B* contains further clarifying information on type of changes requests.

**All IT requests typically fall in one of the three following categories:**

**1) An IT support action;**

**2) a recurring IT requirement; or**
**3) a new IT functional requirement.**

Each of these types is explained below.

**1. Support Action:**

Any USMS user may submit a support request through the USMS IT Help Desk. The Help Desk may be contacted in any of three ways:

1) Online
2) E-mail to ITS.Helpdesk@usdoj.gov
3) Call the Help Desk at 202-307-5200

Support Actions are trouble-shooting issues, primarily handled via phone by the Help Desk. The Help Desk will collect as much information as possible and will either provide the user with a direct answer or give the request to the office responsible for resolving the issue.

Examples of Support Actions are:
a. Account access issues;
b. Hardware failures;
c. Software problems;
d. Telephone problems; and
e. Network desktop connectivity issues

**2. Recurring Requirement**

A requirement is an expressed set of items, tools, processes, or procedures needed to fulfill a need and complete an action. A requirement meets the business needs of the organization and/or individual requestor.

*Recurring Requirements* involve a request for hardware, software or IT services support that is already available within the agency or is on the agency's IT approved configurations or baselines or authorized list of hardware and software.

Recurring Requirements involve hardware or software support that is already available or is on USMS IT approved hardware and software authorized lists.

- Workstations
- Software
- Hardware
- Printers

Recurring requirements follow pre-defined processes and can usually be assigned directly to IT systems support staff for immediate implementation or action. The Help Desk will give the request to the appropriate pre-determined It systems support staff for implementation.

Examples of Recurring Requirements are:

- Installation of Security Patches;
- installation of currently approved COTS of GOTS software;
- installation of currently approved hardware;
- Movement of Equipment;
- Acquisition of Blackberries currently on contract; and
- Access to current IT user Accounts;

**3. New Functional Requirement**

*A new requirement* is defined by a functional need, not a solution. A functional requirement is also defined as a request for service, hardware or software that is not on the current USMS IT approved baseline or authorized list of hardware and software. When the Help Desk cannot provide a direct answer or there isn't an established process or product available, the User's request becomes a New Functional Requirement.

Examples of New Functional Requirements are:

- New software solutions (not on the Baseline);
- Upgraded versions of current software that is being utilized within the USMS;
- Major changes to current enterprise software;
- Acquisition of new type of IT hardware or IT Tools; and

- Requested item or functionality not listed on current IT authorized lists

**RFC Process:** **Procedures for New Functional Requirement**

Changes to IT systems, hardware configurations, or software are initiated through a Request for Change (RFC) process. Any one in the USMS can initiate a request for change via email or a submission of a web based form through the USMS IT Help Desk. The Help Desk may be contacted in any of three ways:

1) Online or through an online requirements form
2) E-mail to ITS.Helpdesk@usdoj.gov
3) Call the Help Desk at 202-307-5200

The IT Help Desk will generate and track a formal request and contact the appropriate It staff that can facilitate and assist the USMS user or office that generated the request. The IT support staff could be involved in one of three roles as it pertains to the request:

- **Program Manager (PM):** an individual responsible for the management of a specific IT formal system, such as the Justice Detainee Information System (JDIS)
- **Account Manager (AM):** an individual assigned responsibly for providing IT service and support to a specific division or mission within the USMS; or a
- **Solution Provider (SP):** an IT staff member that has a unique role in developing an emerging requirement or has expertise in a specific area that is crucial to the development of the new requirement.

The PM/AM/SP then generates a concept proposal which is used to document relevant information, such as specific configuration items, priority of change request, name of requestor, description of change, and the need for change (a sample Concept Proposal form is provided in Appendix C).

The USMS/ITD Configuration control process flow is diagramed and found in Appendix A. The steps identified for this activity typically include:

STEP 1: Submit Request

STEP 1A: Customer Submits Request

*Customer* has a new requirement for a change to their IT environment. This can be any USMS employee who feels they have a need for a change. This is to include, but is not limited to, hardware, software, and communications (voice and data). Change requests will also include requests for IT services.

*Customer* may submit a request for change via a Web Request form, an e-mail , or phone call (202-307-5200) to the Help Desk for any requests.

Proceed to Step 2.

STEP 1B – Internal ITD Personnel Submit Request

*Program Manager (PM), Account Manager (AM) and/or Solution Provider (SP)* personnel initiates request pertaining to operations (such as security patch, software code change, power outage, etc.) or identifies a business problem/opportunity that requires IT as the solution.

PM/AM/SP generates Remedy Ticket.

Proceed to Step 4

STEP 2 – Review and Process Request

*Help Desk* receives the request for requirement from the *Customer* and generates a Remedy Ticket if not already completed.

Proceed to Step 3

STEP 3 – Emergency Request

*Help Desk* staff determines whether the request is an emergency request.

If emergency, proceed to Step 5.

If non-emergency, proceed to Step 9.

STEP 4 – Emergency Request

*PM/AM/SP* staff determines whether the request is an emergency request.

If emergency, proceed to Step 5.

If non-emergency, proceed to Step 11.

STEP 5 – Contact Emergency Approval Personnel

Internal ITD personnel contacts *Emergency Team (CCB and ITD Leadership)* by phone or e-mail.

Proceed to Step 6.

STEP 6 – Approve Emergency Request

*Emergency Team* performs the needs assessment based on the urgency of the turnaround time justified by the business requirement. (Lack of adequate planning does not justify increasing the urgency of processing a request.)

*Emergency Team* Lead should consult with Chief of Information Security Officer

(CISO) to determine if an emergency request presents risks to the posture of the infrastructure/operations prior to implementation. If a risk is present, *Emergency Team* and the assigned ITD personnel need to take the necessary steps to mitigate the risk or obtain a wavier from the CIO to proceed if no mitigation steps are readily available.

If *Emergency Team* Lead approves the request, the team makes an appropriate staff assignment to implement the emergency request. Then Proceed to Step 7.

If *Emergency Team* Lead requires more information about the request, proceed to Step 11.

If *Emergency Team* Lead denies the request, proceed to Step 16.

STEP 7 – Implement Request

*Help Desk, PM, AM or SP* implements the emergency request.

In the event of an emergency change, it is understood that certain documentation (test plans, deployment plans, etc) cannot be produced in advance of the change deployment. Exceptions to documentation requirements will be determined by the *Emergency Team* Lead at the time the request is approved as an emergency request. Required documentation (to include an after action report) will be provided to the *Emergency Team* Lead by assigned ITD personnel who implemented the emergency request within 5 business days after successful completion of the request. The *Emergency Team* Lead is to be kept informed, via telephone, of all status changes of the emergency request. E-mail approvals will be granted as deemed necessary.

If *Help Desk*, proceed to Step 27.

If *PM/AM/SP*, proceed to Step 8.

STEP 8 – Emergency Deployment to Production

*PM/AM/SP* will deploy the requested emergency requirement. All problems with the deployment should be reported to both the Emergency Team. If the deployment fails and the *PM/AM/SP* has to implement rollback procedures, *the PM/AM/SP* will designate which step in the process to return to, in order to correct the problem and re-field the change.

When the request requirement has been successfully implemented, the *PM/AM/SP* should report back to the Account Manager that the change has been deployed successfully.

Proceed to Step 23.

STEP 9 – Pre-approved Production Change

*Help Desk* investigates whether the request is for a pre-approved product/requirement/standard/solution.

If the request is for a pre-approved change, proceed to Step 10.

If the request is for a non-approved change, the *Help Desk* forwards the request to the appropriate Program Manager/Account Manager/Solution Provider. Proceed to Step 11.

STEP 10 – Implement Pre-approved Request

*Help Desk and/or the PM/AM/SP* proceeds to implement the request using guidelines for the pre-approved change.

Proceed to Step 27.

STEP 11 – Develop Concept Proposal/Functional Requirements Document (FRD)

*PM/AM/SP* is responsible for gathering information for the requested requirement. A request must have sufficient information in the needs assessment and benefits/justification and funding authorization from customer for the Functional Control Board (FCB) members to understand the nature, scope, requirements and impact of the requested change. Whenever possible, specific technical information should be included. Supporting documentation, if available, is to be submitted with the request. The Justification should also contain information regarding the impact of declining the request. A request without sufficient information for a decision as to the funding, requirement, impact, or technical implications of a change will be returned without consideration.

A Functional Requirements Document (FRD) may be required to ensure requirements are clearly defined and achieved before work begins. Customer concurrence with the FRD will be necessary prior to work being started.

*PM/AM/SP* should document whether the requested requirement meets the Marshals Enterprise Architecture. If not, *PM/AM/SP* is responsible for consulting with the Chief Technology Officer about the new requirement.

Proceed to Step 12.

STEP 12 – FCB Review

Functional Control Board (*FCB*) conducts a meeting to review documentation for the request and determine the feasibility of the request and ensure funding authority is granted by the customer or internal ITD management to proceed with the request.

Proceed to Step 13.

STEP 13 – Approve Request

If *FCB* approves the request, the FCB makes an appropriate staff assignment to implement the request. Proceed to Step 17.

If *FCB* requires more information about the request, proceed to Step 14.

If *FCB* disapproves/denies the request, proceed to Step 16.

STEP 14 – Identify Stakeholders

FCB requires additional information about the requirement. The PM/AM/SP stands up an Integrated Project Team (*IPT*) with appropriate ITD and customers to clarify the requirements.

Proceed to Step 15.

STEP 15 – Update Concept Proposal/FRD

*IPT* updates the Concept Proposal, FRD and Cost Estimate based on expanded requirements gathering activities.

Proceed to Step 12.

STEP 16 – Deny Request

*FCB* documents justification for denying the request. The reason may be due to budget, personnel availability, technical capability, etc.

Proceed to Step 28.

STEP 17 – SDLC Required

*PM/AM/SP* is responsible for following and delivering a project through the entire SDLC process. System Development Life Cycle (SDLC) process is required if a request needs to involve more than one branch, network upgrades, server upgrades, major software application upgrades, new system proposal, and/or new software application.

If SDLC process is required, proceed to Step 18.

If SDLC process is not required, proceed to Step 21.

STEP 18 – SDLC Design

*PM/AM/SP* team members complete the design phase of the project. The design can

include the Systems Requirements Review (SRR), Preliminary Design Review (PDR) and the Critical Design Review (CDR) activities. Consult the SDLC Manual for additional information.

Once the design is complete, proceed to Step 19.

STEP 19 – ERB Review

Engineering Review Board (*ERB*) conducts a meeting to review the project requirements, design, and plan.

Proceed to Step 20.

STEP 20 – Approve Request

If *ERB* determines the project design and plan are adequate, *ERB* can proceed to approve the request.

If *ERB* determines a request requirement design posses risks to the posture of the infrastructure or operation that cannot be mitigated, *ERB* may elect to seek Chief Information Officer's (CIO's) approval to move forward with the request.

If CIO accepts the security risk, the request moves forward with *ERB's* approval. If CIO does not accept the security risk, additional information and/or redesign may be required to mitigate the risk.

If *ERB* approves the request, proceed to Step 21.

If *ERB* disapproves the request, proceed to Step 18.

STEP 21 – SDLC Development

*PM/AM/SP* performs the necessary development activities such as procurement of software/hardware, evaluate product feasibility, software code change in development, apply patches in development, document procedures to carry out the requirements, etc. Consult the SDLC Manual for additional information.

Proceed to Step 22.

STEP 22 – SDLC Test

*PM/AM/SP and IPT* performs test activities according to the approved project plan. Testing can includes: Development Testing, Integration Test, User Acceptance Testing, Certification & Accreditation Testing, which include user and ITD support staff. A successful security scan may be required. If it is, it will be developed as part of the design and test plans. *PM/AM/SP* is responsible for coordinating with the security staff to accomplish the scanning activities and document scanning results. Consult the SDLC Manual for additional information.

Proceed to Step 23.

STEP 23 – Prepare RFC Package

*PM/AM/SP and ITD Support Staff* document all test results internal, user and support staff acceptance.

*PM/AM/SP* provide test results and other approved documents to CCB for review and approval.

*PM/AM/SP* will develop and provide a coordinated communication plan and deployment plan. Coordination must include all necessary parties, to include ITD branch staffs, customers, and the requesting division/district.

Proceed to Step 24.

STEP 24 – CCB Review and CIO Review

*Configuration Control Board (CCB)* conducts a meeting to verify the development and testing activities have been performed according to the design and test plans, and the risks to the agency are identified for Designated Approving Authority (DAA).

If the CCB recommends approval to deploy, the CCB Chair takes the request to deploy to the *CIO/DAA or D/CIO* for approval to deploy and where appropriate approval to add the solution to the pre-approved production change list.

If the CCB does not recommend deployment, the CCB disapproves with justification.

Proceed to Step 25.

STEP 25 – Approve Request

If non-emergency request, the *CIO/DAA or D/CIO* approves the deployment recommendation and all necessary documentation, proceed to Step 26.

If emergency request follow-up, the *CIO/DAA or D/CIO* approves all necessary documentation, proceed to Step 29.

If *CCB* disapproves the request, the CCB will recommend which step the PM/AM/SP should proceed to for resolving the concerns raised. Proceed to Step 18, 22 or 23 based on CCB guidance.

STEP 26 – Deploy to Production

*PM/AM/SP* will deploy the request requirement, including converting/migrating legacy systems/data, and training users. All problems with the deployment should be

reported to both the respective Functional Managers. If the deployment fails and *PM/AM/SP* has to implement rollback procedures, *PM/AM/SP* will designate which step in the process to return to, in order to correct the problem and re-field the change. *PM/AM/SP* should also inform Account Manager of unsuccessful deployment during the process.

When the request requirement has been successfully implemented, the *PM/AM/SP* should report back to the Account Manager that the change has been deployed successfully. If the deployment is unsuccessful, the request reverts to the appropriate step in the workflow process to correct the problem and then continues from that point forward to complete the change.

If the request is a reoccurring requirement that is to become a pre-approved change, the *PM/AM/SP* will ensure all lessons learned are added to/incorporated into the pre-approved change documentation package.

If the deployment is successful, proceed to Step 29.

STEP 27 – Close Request

*Help Desk* verifies with the Customer that the change is operating in production as requested. *Help Desk* documents verification and validate of the implementation in the ticket. The Customer's validation will be documented in the ticket. The *Help Desk* closes the request ticket.

STEP 28 – Close Request

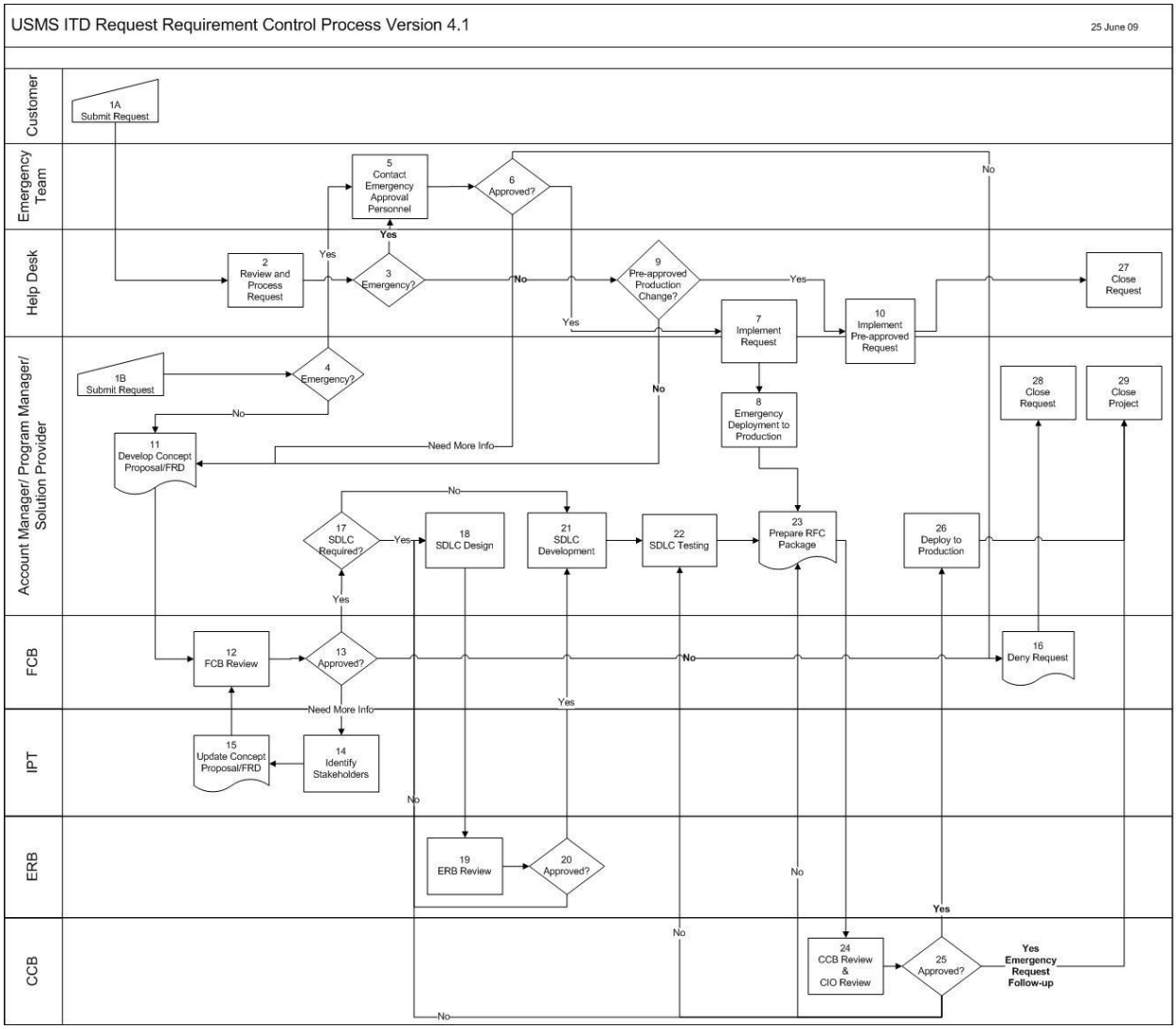
*PM/AM/SP* informs Customer of denied request and closes request.

STEP 29 – Close Project

*PM/AM/SP* closes completed project as requested per Request Requirement Control Process or per SDLC process. Necessary documentation such as system description document and system security plan may need to be updated prior to project closure. Upon project closure, *PM/AM/SP* is responsible for notifying Chief Technology Officer to update the Enterprise Architecture artifacts of the new approved product/requirement/standard.

**APPENDIX A** **ITD Change Control Process**

**For larger PDF version of the flow chart process**




## Appendix B: RFC: Categories of IT System Changes

## APPENDIX C – Sample Concept Proposal

For a Word Document format version

**United Statess Marshals Service**
**Information Technology Division**

Project Initiation
Concept Proposal Document

## 1.0 TITLE OF PROJECT

(TITLE SHOULD CARRY OVER TO PAGE 2)

## 1.1 ORIGINATOR

| Division | Branch | Name |
|---|---|---|
| | | |

| 1.2 ORIGINATION DATE | 1.3 REQUESTED COMPLETION DATE |
|---|---|
| | |

## ACTIONS DETERMINED BY THE FCB

| | | |
|---|---|---|
| Solution Provider | | |
| Applicable Certification and Accreditation (C&A) System | | |
| Class of Project<br>(see Section 14) | ☐ New System Development<br>☐ System Development Upgrade<br>☐ System Dev Bug Fix/Patch<br>☐ New/Major Upgrade COTS/non-USMS GOTS<br>☐ COTS/non-USMS GOTS Minor Upgrade<br>☐ New Network/Hardware/Network Hardware<br>☐ OTHER: | ☐ Network/Hardware/Network Hardware Change/Upgrade<br>☐ Firewall Port Change<br>☐ Maintenance Outage Request<br>☐ Telephone<br>☐ Office Renovation/Move/ Relocation |
| Additional Resources | | |
| SDLC Management Process | Design/ERB ☐ | Dev/Test/CCB ☐ |
| Documentation Requirements | | |
| Priority | | |

## 2.0 DESCRIPTION OF PROJECT

### 2.1 Mission/Goals Investment Supports

### 2.2 Existing Structure

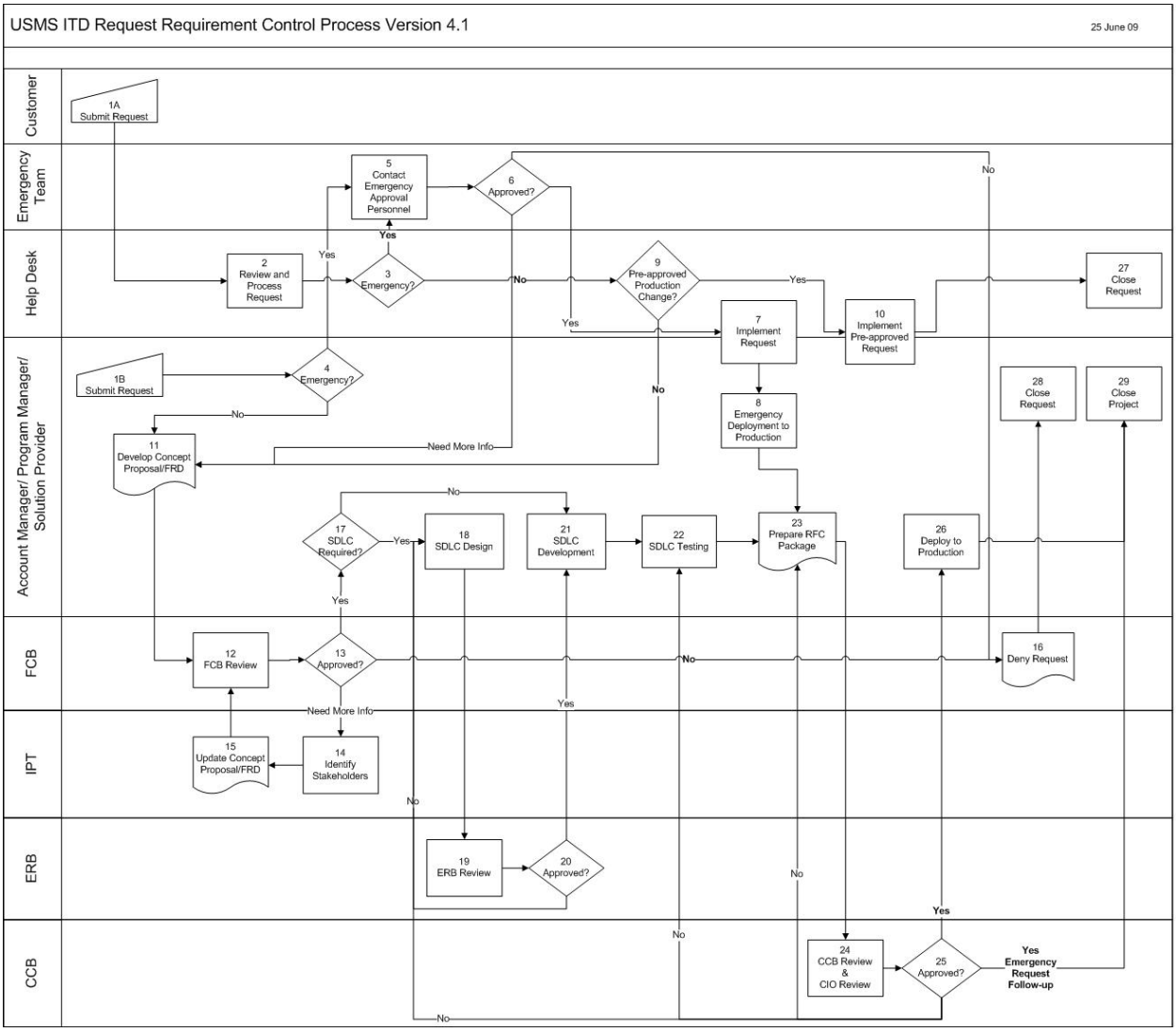
### 2.3 Benefits

### 2.4 Warranted Investment

### 2.5 Funding Level

### 2.6 Funding Source

# ITD Change Control Process



# Appendix B: RFC: Categories of IT System Changes

**Explanation of Project Categories**

| Category of Project | Definitions and Examples |
|---|---|
| **Software** | |
| New Systems Development | The first release or version of a prominent USMS application built from any combination of COTS, GOTS and custom developed code. Prioritization of the project will include consideration of the size and distribution of the user community, availability requirement related to mission critical availability, and stability demands regarding level of acceptable risk. |
| Systems Development Upgrade | A major software release of a USMS application consisting of new functionality, major interface changes, core product changes, or any combination thereof. These changes are typically denoted by an increase to the version number to the left of the decimal point (example: v1.3 to v2.0) |
| Systems Development Bug Fix/Patch | A minor software release of a USMS application consisting of bug fixes, minor functionality changes impacting single modules of code, changes to static content, or any combination thereof. For minor releases involving anything other than bug fixes, the version is denoted by an increase to the version number to the right of the decimal point (example: v1.3 to v1.4) For minor releases involving only bug fixes, the rightmost decimal will be increased to denote a revision to an existing release. (Example: v1.3. to v1.3.1) |
| New/Major Upgrade COTS/non-USMS GOTS Installation | The first introduction of a Commercial off the Shelf product not requiring custom developed code or modifications beyond infrastructure integration and configuration tasks. Only products marketed by a vendor, supplied with installable executable files, and delivered with complete system documentation and installation manuals will be considered true COTS products. Products falling into this category include: Operating systems, applications, and desktop or server tools. (i.e., Microsoft Windows XP, Microsoft Exchange, Adobe Photoshop, etc.) The complexity level of the product will determine the level of "Case Specific" Items required.<br><br>A COTS product release consisting of new functionality, major interface changes, core product changes, or any combination thereof. These changes are typically denoted by an increase to the version number to the left of the decimal point (example: v1.3 to v2.0) |
| COTS/non-USMS GOTS Minor Upgrade | A minor COTS/GOTS release consisting of bug fixes, minor functionality changes impacting single modules of code, changes to static content, or any combination thereof. For minor releases involving anything other than bug fixes, the version is denoted by an increase to the version number to the right of the decimal point (example: v1.3 to v1.4) For minor releases involving only bug fixes, the rightmost decimal will be increased to denote a revision to an existing release. (Example: v1.3. to v1.3.1) Service packs, VPR patches, and hot fixes are not considered version upgrades unless the vendor markets the product as an upgrade to the version number. |
| New Network/Hardware/Network Hardware | New hardware instance. Examples include: new server, network device, new storage, new facility, IDS equipment, voice over IP, audio/visual systems, and peripheral devices beyond printers, scanners, and multi-function devices. |
| Network/Hardware/Network Hardware Change/Upgrade | A change to core infrastructure; network, server, or storage topology; enterprise routing or switching; or facility location/configuration. Examples of upgrades requiring formal approval are: replacement of a server for capacity or |

| | |
|---|---|
| | performance issues, change of storage platform, and replacement of core network devices or major distribution components.<br><br>Changes attributed to main unit or component failure, media change, cabling, or trivial reconfigurations are maintenance outages. |
| Maintenance Outage Request | Maintenance outage requests are outages related to repair, update, or minor configuration changes. Items in this category are those with impact to internal or external users. Reasons for outage requests are: patch installation, database or application maintenance, re-cabling, and changes to systems requiring one or more software or services to be stopped for any period of time. |
| Firewall Port Open/ Close | Opening of firewall ports, closing of firewall ports, changes to allowed protocols, changes to access control lists, and changes to source and destination addresses. |
| Telephone | TBD |
| Office Renovations/Move/ Relocation | TBD |

United States Marshals Service POLICY DIRECTIVES

**INFORMATION RESOURCES MANAGEMENT**

# Request for Change (RFC)

## Frequently Asked Questions on the RFC Process

**Do I still use the USM Form 168, System Change Request/Request for Change Form?**

**Use of the SCR Form has been discontinued.** The IT representative will complete the Request for Change and submit it to the appropriate Program Manager.

**What is an incomplete submission? How do I know what information to include?**

An RFC must have sufficient information in the needs assessment and benefits/justification for the PM to understand the nature, scope, requirements and impact of the requested change. Whenever possible, specific technical information should be included. Supporting documentation, if available should be submitted with the RFC. The Justification section should also contain information regarding the impact of declining the RFC. An RFC without sufficient information for a decision as to the requirement, impact, or technical implications of a change will be returned without consideration.

**What is the due date? What if I need something completed by a very specific date.**

The due date field on the RFC form represents the customer's desired implementation date. It should be filled out; however, it serves as an advisement to the IT Staff working with the RFC, and should not be considered authoritative. The PM will communicate dates as they are available to the requester based on information received from IT staff during each approval section.

If a change must be completed within a certain time frame, please include that time frame within the needs assessment (Why it needs to be completed within a certain time frame) and in the justification system, explain the impact of not completing the change by the desired date.

**What is the Priority field for?**

The Priority field represents the turn around time justified by the business requirement for the NEEDS ASSESSMENT approval by the PM. Following an approved NEEDS ASSESSMENT, the RFC is distributed to Operational supervisors and staff for an anticipated level of effort. At the conclusion of operational input, a due date can be determined.

## 12.7.4 PRIVACY IMPACT ASSESSMENTS

**A.** **Purpose:** This directive establishes policy for conducting a Privacy Impact Assessment (PIA) on USMS computer and telecommunications systems.

**B.** **Responsibilities:** Privacy Impact Assessment (PIA) Reviewing Official: Responsible to the SPM for overseeing the PIA process at USMS and reviewing each PIA conducted by the USMS. The USMS FOIA/Privacy Act Officer shall serve as the PIA Official for the USMS.

**C.** **Policy:** Ensuring USMS systems and information are secure is a top priority. USMS employees must be sure that their actions compromise neither the security of USMS computer and telecommunications systems nor the data (including privacy information) contained in them. (Note: Additional IT security policies and procedures may be found in USMS Publication 64, *Requirements Specifications for Special Purpose and Support Space*.)

1. **Background:** Rapid advancements in computer technology make it possible to store and retrieve vast amounts of data quickly and efficiently. These advancements have raised concerns about the impact of large computerized information systems on the privacy of individuals. To address these concerns, PIAs are to be conducted as appropriate to ensure that the privacy concerns of individuals are properly accounted for as systems are developed.

2. **New Information Systems:** A PIA shall be conducted for any new major information system which meets any of the following criteria:

   a. Contains sensitive information regarding individuals (e.g., medical information), regardless of the number of records in the system.

   b. Uses new techniques and/or technology to manipulate existing data about individuals in a way that such data is readily retrievable.

   c. Collects and maintains personal information about individuals that has not previously been collected and maintained by the USMS.

3. **Modifications to Existing Systems:** A PIA shall be conducted if the major system to be modified substantively and directly affects system data on individuals.

4. **Written Assessment:** The PIA shall be a written assessment of the impact attributable to the proposed system or modification of an existing system. Written USMS PIA assessments may be modeled on published government agency best practices for PIAs (e.g., IRS).

5. **PIA Reviewing Official Approval:** A PIA is to be performed as early as possible during the development of a new major system (or major system modification), ideally when requirements are being analyzed and decisions are being made about data usage and

system design. At the time funds are requested for implementation of the system, approval from the USMS PIA reviewing official must be obtained.

## 12.7.5 PORTABLE REMOTE COMPUTING SYSTEMS PROCEDURES

**A. General Considerations:**

1. The normal execution of the United States Marshals Service (USMS) mission necessitates the use of portable remote computing systems such as laptop computers, notebook computers, handheld computing devices, tablet computers, paging devices, and cellular communication devices. For the purpose of this document, all such mobile devices are considered part of portable remote computing systems and are subject to the requirements contained herein.

2. The inherent wireless, mobile nature of portable remote computing systems presents unique, universally present security risks associated with the devices themselves as well as the data contained on them. Special precautions must be exercised to safeguard the devices and the information they contain to ensure the uniform, secure, uninterrupted execution of the mission of the USMS.

**B. Applicable Guidelines:** Mobile devices will be handled with common sense and with security in mind by those to whom they are assigned. All mobile devices used to connect to USMS systems and the data contained on them are considered the property of the USMS and thus must be purchased and provided by the USMS. Mobile devices will be configured by ITS professionals. Disposal of mobile devices must be done in accordance with government regulations.

1. **Mobile Device Hardware/Software:** Mobile device hardware shall be construed as being the device itself or any part that is attached to the device to enhance its use. Mobile device software shall be construed as including any data or coding that is loaded onto a computer storage device.

2. **Mobile Device Data:** Safeguarding of all USMS data is the responsibility of the person to whom the mobile device is assigned. No government credit card numbers, calling card numbers, access ID's, passwords, etc. may be stored on USMS mobile devices.

   a. No witness protection data, or data classified at the "NSI Level", may be stored on a mobile device.

   b. Sensitive data should be left in a USMS office unless specifically and temporarily being required outside the office.

   c. Any data that must be transmitted shall be encrypted in accordance with DOJ and USMS policy and procedures.

   d. Data stored on removable media (diskettes, ZIP disks, CD, etc) shall be treated with the same discretion as that stored on the mobile device itself.

   e. Loading inappropriate material onto USMS mobile devices is not permitted. Inappropriate material shall be considered to be, but not limited to, sexually

explicit material, unlicensed software, data with a security clearance that exceeds the user's clearance, software that might create a vulnerability in the USMS network, etc.

3. **Preventing Mobile Device Theft:** Be deliberate…never assume your mobile device is safe. Protect your device and the data on it as you would protect your personal valuables (e.g., wallet, credit card, jewelry).

   a. Mobile devices containing USMS data shall not be checked as baggage on public transportation such as airlines, buses, ocean liners, etc.

   b. Do not leave a mobile device unattended in public places, including telephone booths, hotel lobbies, rest rooms, etc.

   c. If left in a vehicle, place mobile device in locked trunk or out of sight.

   d. Properly secure your mobile device in a hotel room or office whenever feasible (e.g., lock onto a stationary object).

4. **Reporting Mobile Device Theft:** In the event a mobile device is lost or stolen, the following protocol shall be strictly adhered to:

   a. Notify your supervisor and ITS immediately. ITS will assess the level of the threat or damage and advise.

   b. Notify local law authorities immediately and request an incident number. Make no mention regarding the data on the device or the security level of the data.

   c. Survey the situation to ensure security of any additional hardware or equipment.

   d. mmediately begin to document the activities leading up to the incident. Include as many details (data on the device, times, dates, locations, etc) as possible.

   e. Notify your local property custodian.

**C. Laptops:**

1. **Laptop Encryption:** Once the laptop is configured, it will be loaded with the encryption software authorized by USMS. The encryption software required by DOJ will be installed on every JCON-issued laptop. All legacy laptop systems must be modified within 90 days after issuance of this procedure to include DOJ-required encryption.

2. **Laptop Connections:** A laptop may not be connected via land or cellular methods to outside commercial dial-up networks (e.g., AOL, CompuServe, etc.) without express ITS approval.

**D. Personal Digital Assistant (PDA) Devices:**

1. **Key Functional Requirements:** The main PDA functions used by the USMS are:

   a. Capability to synchronize with a desktop or laptop computer.

   b. Capability to save and backup information.

   c. Capability to add, update, delete contact information.

d. Capability to add, update, delete tasks.

e. Capability to perform event scheduling.

f. E-mail (Synchronize with Desktop/Laptop).

2. **USMS Standard:** The established PDA standards are available on the USMS ITS Intranet website. PDA units must only be able to synch to a JCON workstation via a cradle, and must not sync/exchange data to any device outside of the USMS JCON workstation. All PDAs connected to the USMS MNET must be Government owned and trackable via serial number.

3. **Security Considerations:** PDA security should be a serious concern for every handheld device user. PDAs are very portable, which makes them easy targets for thieves and are easily misplaced or lost. The USMS requires that ITS-approved anti-virus protection software and encryption software be installed on all PDAs so that data is encrypted and security risks are mitigated. The certified software for the PC should be installed by an ITS staff member and be accessible to the assigned user only.

   a. Data security begins with basic password protection for locking access to a handheld computer and securing data.

   b. **Law Enforcement Sensitive Information:** Users are strongly discouraged from using PDAs for receiving, transmitting, or storing law enforcement sensitive data on PDAs. Supervisors should carefully weigh the dangers of potential loss or disclosure of sensitive information against the convenience of portable computing. To the extent that the user's supervisor authorizes such use:

      1) Anti-virus protection must be installed and kept up-to-date, data must be encrypted, and access should be password protected.

      2) If data is transmitted during synchronization, then proper user/device authentication must be ensured before transmitting data and an audit trail maintained.

      3) If data is transmitted wirelessly, then proper user/device authentication must be ensured before transmission, data encrypted during the transmission, and an audit trail maintained.

      4) To protect data if the PDA is lost or stolen, utilize user ID and password level security, user/device validation during synchronization, and encryption of the data stored on the PDA.