



**Office of the Chief Information Officer (OCIO)  
United States Patent and Trademark Office (USPTO)**

## ***USPTO IT SECURITY HANDBOOK***

**June 2008**

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

## **1. PURPOSE**

The purpose of this *USPTO IT Security Handbook* is to document security policies and procedures in accordance with Federal government mandated requirements based on standards and procedures issued by the Office of Management and Budget (OMB), the Department of Commerce (DOC), the United States Patent and Trademark Office (USPTO), and the National Institute of Standards and Technology (NIST).

## **2. AUTHORITY**

This policy is issued pursuant to:

- The Federal Information Management Security Act of 2002 (FISMA).
- USPTO IT Security Policy Management Policy.

## **3. SCOPE**

The provisions of this policy apply to all USPTO employees and contractor employees, accessing or using USPTO data, and to contractor employees providing services to the USPTO who use USPTO Automated Information Systems (AIS), data and networks. It applies to all USPTO AIS or resources, independent of size. Additionally, this policy applies to all types of media used to store USPTO personally identifiable information (PII) which include, but are not limited to: hard drives, CDs, DVDs, other magnetic media such as floppy disks, and solid-state media (flash memory, memory stick, Universal Serial Bus (USB) flash drive, thumb drive etc.). Finally, it applies to all media output (soft and hard-copy) that contain USPTO PII.

This policy also applies to AIS and equipment, including network devices, operated and used by contractor employees, guest researchers, collaborators, and other federal agencies to carry out the USPTO mission, whether or not they are owned, leased, or on government property. It shall be explicitly addressed in all IT procurement activities.

This policy pertains to both electronic, hard-copy (paper) records and microfilm.

## **4. APPLICABILITY**

The *USPTO IT Security Handbook* applies to all USPTO personnel and contractors who use or access USPTO Information Technology (IT) systems.

## **5. SUMMARY OF CHANGES**

The OCIO IT Security Management Group must approve all changes to this Handbook. Changes are summarized in the Record of Changes on page ii.

## **6. RECOMMENDATIONS**

Comments concerning this handbook should be forwarded to the USPTO OCIO ITSMG.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

## **7. APPROVAL**

All USPTO information technology documents should be written in accordance with this handbook and shall be approved by the designated management officials identified in this handbook.

## **8. EXCEPTIONS**

Please refer to the waiver process as defined in the USPTO IT Security Handbook.

## **9. EFFECTIVE DATE**

This policy is effective on the date it is signed. The anticipated review date is one year from the date of approval.

---

Approved by:  
Wendy Garber  
Acting Chief Information Officer

---

Date Signed

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

## Record of Changes

<b>Change Number</b>	<b>Date of Change</b>	<b>Sections Changed</b>	<b>Description</b>	<b>Person Approving Change</b>
PPC-ITSecHandbook-06-30-v.5.doc	04/26/2007	All	Initial Submission	Quentin Robinson
PPC-USPTO IT Security Handbook-v.6.doc	07/18/2007	All	Revised all sections based on renaming remaining? LOE as per USPTO TOM	Quentin Robinson
v.7	8/23/07	All	New org structure incorporated more minor edits.	Quentin Robinson
v.8	10/3/07	All	General editing	Quentin Robinson
V2.5	12/20/07	All	General Editing	Quentin Robinson
V2.8.1	6/16/08	Signature	Changed Approving Authority	Katherine Queen

This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.

## Table of Contents

<b>1</b>	<b>INTRODUCTION .....</b>	<b>1</b>
1.1	Background .....	1
1.2	Policy.....	2
1.3	Roles and Responsibilities.....	2
<b>2</b>	<b>INFORMATION TECHNOLOGY SECURITY PROGRAM MANAGEMENT .....</b>	<b>15</b>
2.1	Purpose .....	15
2.1.1	<i>Security Categorization (Sensitivity Rating Level) .....</i>	<i>16</i>
2.1.2	<i>Security Objectives – Confidentiality/Integrity/Availability .....</i>	<i>16</i>
2.1.2.1	<i>Confidentiality .....</i>	<i>16</i>
2.1.2.2	<i>Integrity.....</i>	<i>17</i>
2.1.2.3	<i>Availability.....</i>	<i>17</i>
2.2	Policy Development and Maintenance .....	18
2.2.1	<i>IT Security Standards .....</i>	<i>18</i>
2.2.2	<i>Security Bulletins .....</i>	<i>18</i>
2.2.3	<i>Baseline System Security Requirements.....</i>	<i>19</i>
2.3	Program and Budgets.....	20
2.4	Security Performance Measures and Metrics .....	20
2.5	Reporting .....	20
<b>3</b>	<b>MANAGEMENT CONTROLS.....</b>	<b>21</b>
3.1	Planning .....	21
3.1.1	<i>Purpose/Requirements .....</i>	<i>21</i>
3.1.2	<i>Policy .....</i>	<i>22</i>
3.1.2.1	<i>Security Planning.....</i>	<i>22</i>
3.1.2.2	<i>System Security Plan.....</i>	<i>22</i>
3.1.2.3	<i>System Security Plan Update .....</i>	<i>23</i>

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

<b>3.1.2.4</b>	<i>Rules of Behavior</i> .....	24
<b>3.1.2.5</b>	<i>Privacy Impact Assessment</i> .....	25
<b>3.2</b>	<b>System and Services Acquisition</b> .....	<b>25</b>
3.2.1	<i>Purpose/Requirements</i> .....	25
3.2.2	<i>Policy</i> .....	27
<b>3.2.2.1</b>	<i>System and Services Acquisition</i> .....	27
<b>3.2.2.2</b>	<i>Allocation of Resources</i> .....	27
<b>3.2.2.3</b>	<i>Life Cycle Management</i> .....	27
<b>3.2.2.4</b>	<i>Acquisitions</i> .....	28
<b>3.2.2.5</b>	<i>System Documentation</i> .....	31
<b>3.2.2.6</b>	<i>Software Usage Restrictions</i> .....	32
<b>3.2.2.7</b>	<i>User Installed Software</i> .....	33
<b>3.2.2.8</b>	<i>Security Engineering Principles</i> .....	33
<b>3.2.2.9</b>	<i>External Information System Services</i> .....	34
<b>3.2.2.10</b>	<i>Developer Security Testing</i> .....	34
<b>3.3</b>	<b>Risk Assessment</b> .....	<b>34</b>
3.3.1	<i>Purpose/Requirements</i> .....	34
3.3.2	<i>Policy</i> .....	35
<b>3.3.2.1</b>	<i>Risk Assessment</i> .....	35
<b>3.3.2.2</b>	<i>Security Categorization</i> .....	35
<b>3.3.2.3</b>	<i>Risk Assessment Reports</i> .....	36
<b>3.3.2.4</b>	<i>Vulnerability Scanning</i> .....	36
<b>3.4</b>	<b>Certification, Accreditation, and Security Assessments</b> .....	<b>37</b>
3.4.1	<i>Purpose/Requirements</i> .....	37
3.4.2	<i>Policy</i> .....	38
<b>3.4.2.1</b>	<i>Certification, Accreditation, and Security Assessment</i> .....	38
<b>3.4.2.2</b>	<i>Certification Testing</i> .....	38

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

3.4.2.3	System Interconnection/Information Sharing .....	39
3.4.2.4	Security Certification.....	40
3.4.2.5	Plan of Action and Milestones.....	40
3.4.2.6	Security Accreditation .....	40
3.4.2.7	Continuous Monitoring.....	41
<b>4</b>	<b>OPERATIONAL CONTROLS.....</b>	<b>42</b>
<b>4.1</b>	<b>Personnel Security.....</b>	<b>42</b>
4.1.1	Purpose/Requirements .....	42
4.1.2	Policy .....	43
4.1.2.1	Personnel Security.....	43
4.1.2.2	Position Categorization.....	44
4.1.2.3	Personnel Screening (Background Investigations) .....	44
4.1.2.4	Personnel Separation or Transfer.....	44
4.1.2.5	Access Agreements.....	45
4.1.2.6	Third-Party Personnel Security.....	45
4.1.2.7	Personnel Sanctions.....	45
<b>4.2</b>	<b>Awareness and Training.....</b>	<b>46</b>
4.2.1	Purpose/Requirements .....	46
4.2.2	Policy .....	47
4.2.2.1	Security Awareness and Training .....	47
4.2.2.2	Security Training and Awareness .....	47
4.2.2.3	Security Training Records.....	48
<b>4.3</b>	<b>Physical and Environmental Protection .....</b>	<b>49</b>
4.3.1	Purpose/Requirements .....	49
4.3.2	Policy .....	50
4.3.2.1	Physical and Environmental Protection.....	50
4.3.2.2	Physical Access.....	51

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

<i>4.3.2.3</i>	<i>Access Control for Display Medium</i>	<i>52</i>
<i>4.3.2.4</i>	<i>Visitor Control</i>	<i>52</i>
<i>4.3.2.5</i>	<i>Equipment Security</i>	<i>52</i>
<i>4.3.2.6</i>	<i>Fire Prevention</i>	<i>53</i>
<i>4.3.2.7</i>	<i>Water Damage Protection</i>	<i>53</i>
<i>4.3.2.8</i>	<i>Supporting Utilities</i>	<i>53</i>
<b>4.4</b>	<b>Incident Response</b>	<b>54</b>
<i>4.4.1</i>	<i>Purpose/Requirements</i>	<i>54</i>
<i>4.4.2</i>	<i>Policy</i>	<i>55</i>
<i>4.4.2.1</i>	<i>Incident Response</i>	<i>55</i>
<i>4.4.2.2</i>	<i>Incident Response Training</i>	<i>55</i>
<i>4.4.2.3</i>	<i>Incident Response Testing and Exercises</i>	<i>56</i>
<i>4.4.2.4</i>	<i>Incident Handling and Monitoring</i>	<i>56</i>
<i>4.4.2.5</i>	<i>Incident Reporting and Response</i>	<i>57</i>
<b>4.5</b>	<b>Media Protection</b>	<b>60</b>
<i>4.5.1</i>	<i>Purpose/Requirements</i>	<i>60</i>
<i>4.5.2</i>	<i>Policy</i>	<i>61</i>
<i>4.5.2.1</i>	<i>Media Protection</i>	<i>61</i>
<i>4.5.2.2</i>	<i>Sensitive Information Handling</i>	<i>61</i>
<i>4.5.2.3</i>	<i>Media Access and Control</i>	<i>62</i>
<i>4.5.2.4</i>	<i>Media Storage and Transport</i>	<i>62</i>
<i>4.5.2.5</i>	<i>Sanitization and Disposal of Information</i>	<i>62</i>
<b>4.6</b>	<b>System and Information Integrity</b>	<b>63</b>
<i>4.6.1</i>	<i>Purpose/Requirements</i>	<i>63</i>
<i>4.6.2</i>	<i>Policy</i>	<i>63</i>
<i>4.6.2.1</i>	<i>System and Information Integrity</i>	<i>63</i>
<i>4.6.2.2</i>	<i>Flaw Remediation</i>	<i>64</i>

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

4.6.2.3	<i>Malicious Code Protection</i>	64
4.6.2.4	<i>Information System Monitoring Tools and Techniques</i>	65
4.6.2.5	<i>Security Alerts and Advisories</i>	65
4.6.2.6	<i>Spam Protection</i>	65
4.6.2.7	<i>Information Input/Output and Error Handling</i>	65
<b>4.7</b>	<b>Maintenance</b>	<b>66</b>
4.7.1	<i>Purpose/Requirements</i>	66
4.7.2	<i>Policy</i>	66
4.7.2.1	<i>System Maintenance</i>	66
4.7.2.2	<i>Controlled Maintenance</i>	67
4.7.2.3	<i>Maintenance Tools</i>	67
4.7.2.4	<i>Remote Maintenance</i>	67
<b>4.8</b>	<b>Contingency Planning</b>	<b>67</b>
4.8.1	<i>Purpose/Requirements</i>	67
4.8.2	<i>Policy</i>	69
4.8.2.1	<i>Contingency Planning</i>	69
4.8.2.2	<i>Contingency Plan</i>	70
4.8.2.3	<i>Contingency Training</i>	70
4.8.2.4	<i>Contingency Plan Testing and Exercises</i>	70
4.8.2.5	<i>Alternate Storage and Processing Sites</i>	70
4.8.2.6	<i>Telecommunications Services</i>	70
4.8.2.7	<i>Information System Backup</i>	71
4.8.2.8	<i>Information System Recovery and Reconstitution</i>	71
<b>4.9</b>	<b>Configuration Management</b>	<b>71</b>
4.9.1	<i>Purpose/Requirements</i>	71
4.9.2	<i>Policy</i>	72
4.9.2.1	<i>Configuration Management</i>	72

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

<b>4.9.2.2</b>	<i>Baseline Configuration</i>	72
<b>4.9.2.3</b>	<i>Configuration Change Control</i>	72
<b>4.9.2.4</b>	<i>Monitoring Configuration Changes</i>	72
<b>4.9.2.5</b>	<i>Access Restrictions for Change</i>	72
<b>4.9.2.6</b>	<i>Configuration Settings</i>	73
<b>4.9.2.7</b>	<i>Least Functionality</i>	73
<b>4.9.2.8</b>	<i>Information System Component Inventory</i>	73
<b>5</b>	<b>TECHNICAL CONTROLS</b>	<b>74</b>
<b>5.1</b>	<b>Identification and Authentication</b>	<b>75</b>
5.1.1	<i>Purpose/Requirements</i>	75
5.1.2	<i>Policy</i>	76
5.1.2.1	<i>Identification and Authentication</i>	76
5.1.2.2	<i>User Identification and Authentication</i>	76
5.1.2.3	<i>Device Identification and Authentication</i>	76
5.1.2.4	<i>Identifier Management</i>	76
5.1.2.5	<i>Authenticator Management and Feedback</i>	76
5.1.2.6	<i>Cryptographic Module Authentication</i>	77
<b>5.2</b>	<b>Access Control</b>	<b>77</b>
5.2.1	<i>Purpose/Requirements</i>	77
5.2.2	<i>Policy</i>	79
5.2.2.1	<i>Access Control</i>	79
5.2.2.2	<i>Account Management</i>	80
5.2.2.3	<i>Access Enforcement</i>	80
5.2.2.4	<i>Information Flow Enforcement</i>	80
5.2.2.5	<i>Separation of Duties</i>	80
5.2.2.6	<i>Least Privilege</i>	81
5.2.2.7	<i>Automatic Account Lockout</i>	81

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

<i>5.2.2.8</i>	<i>System Use Notification</i>	81
<i>5.2.2.9</i>	<i>Automatic Session Lockout</i>	81
<i>5.2.2.10</i>	<i>Session Termination</i>	81
<i>5.2.2.11</i>	<i>Supervision and Review</i>	81
<i>5.2.2.12</i>	<i>Permitted Actions without Identification and Authentication</i>	82
<i>5.2.2.13</i>	<i>Remote Access</i>	82
<i>5.2.2.14</i>	<i>Wireless Access</i>	82
<i>5.2.2.15</i>	<i>Access Control for Portable and Mobile Devices</i>	83
<i>5.2.2.16</i>	<i>Use of External Information Systems</i>	84
<b>5.3</b>	<b>Audit and Accountability</b>	<b>84</b>
5.3.1	<i>Purpose/Requirements</i>	84
5.3.2	<i>Policy</i>	85
<i>5.3.2.1</i>	<i>Audit and Accountability</i>	85
<i>5.3.2.2</i>	<i>Auditable Events</i>	85
<i>5.3.2.3</i>	<i>Audit Storage Capacity</i>	85
<i>5.3.2.4</i>	<i>Response to Audit Processing Failures</i>	85
<i>5.3.2.5</i>	<i>Audit Monitoring, Analysis, and Reporting</i>	85
<i>5.3.2.6</i>	<i>Audit Reduction and Report Generation</i>	85
<i>5.3.2.7</i>	<i>Time Stamps</i>	86
<i>5.3.2.8</i>	<i>Protection of Audit Information</i>	86
<i>5.3.2.9</i>	<i>Audit Record Retention</i>	86
<b>5.4</b>	<b>System and Communications Protection</b>	<b>86</b>
5.4.1	<i>Purpose/Requirements</i>	86
5.4.2	<i>Policy</i>	87
<i>5.4.2.1</i>	<i>System and Communications Protection</i>	87
<i>5.4.2.2</i>	<i>Application Partitioning</i>	88
<i>5.4.2.3</i>	<i>Information Remnance</i>	88

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

<i>5.4.2.4 Denial of Service Protection</i>	88
<i>5.4.2.5 Boundary Protection</i>	88
<i>5.4.2.6 Transmission Integrity and Confidentiality</i>	88
<i>5.4.2.7 Network Disconnect</i>	88
<i>5.4.2.8 Cryptographic Key Establishment and Management</i>	89
<i>5.4.2.9 Public Access Protections</i>	89
<i>5.4.2.10 Collaborative Computing</i>	89
<i>5.4.2.11 Public Key Infrastructure</i>	89
<i>5.4.2.12 Mobile Code</i>	90
<i>5.4.2.13 Communications Security (Voice/Data (Facsimile/VoIP))</i>	90
<i>5.4.2.14 Secure Name/Address Resolution Service (Authoritative Source)</i>	91
<i>5.4.2.15 Session Authenticity</i>	91
<b>6 POLICY ENFORCEMENT</b>	<b>92</b>
6.1 Inspections	93
<b>7 WAIVERS</b>	<b>94</b>
Appendix A References	A-1
Appendix B Acronyms and Abbreviations	B-1
Appendix C GLossary	C-1

This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.

## List of Tables

Table 3-1 Planning Controls.....	22
Table 3-2: System and Services Acquisition Controls.....	26
Table 3-3: Required System Security Documentation .....	32
Table 3-4: Risk Assessment Controls .....	35
Table 3-5: Certification and Accreditation Controls.....	38
Table 4-1: Personnel Security Controls .....	43
Table 4-2: Awareness and Training Controls .....	46
Table 4-3 Physical and Environmental Controls .....	50
Table 4-4 Incident Response Controls .....	55
Table 4-5 Media Protection Controls .....	61
Table 4-6 System and Information Integrity Controls .....	63
Table 4-7: Maintenance Controls .....	66
Table 4-8 Contingency Planning Controls .....	69
Table 4-9 Configuration Management Controls.....	71
Table 5-1 Identification and Authentication Controls .....	75
Table 5-2 Access Controls .....	78
Table 5-3 Audit and Accountability Controls.....	84
Table 5-4 System and Communications Protection Controls .....	87

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

## **List of Figures**

<b>Figure 3-1: IT Security and Capital Planning Regulations and Guidance .....</b>	<b>26</b>
<b>Figure 3-2: NIST and USPTO SDLC Mapping.....</b>	<b>28</b>
<b>Figure 3-3: Flowchart of Key Information Security Decisions in the Acquisition Process.....</b>	<b>30</b>
<b>Figure 3-4: IT Security and Capital Planning .....</b>	<b>31</b>
<b>Figure 4-1: USPTO Incident Report Process .....</b>	<b>58</b>
<b>Figure 5-1: Technical Security Controls.....</b>	<b>74</b>
<b>Figure 6-1: USPTO Incident Reporting Process Non-Conformance .....</b>	<b>92</b>

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

# **1 INTRODUCTION**

## **1.1 Background**

The Federal Information Security Management Act of 2002, Public Law 107-347, provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, and defines “adequate security” as security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost effective management, personnel, operational and technical controls. Therefore, all USPTO programs must include at a minimum the following controls in their General Support System (GSS) and Major Applications (MA):

- Responsibility for Security through implementation of the roles and responsibilities as identified later in this Handbook.
- System Security Plan (SSP)
- Certification of Security Controls
- Authorization to Operate

*Federal Information Processing Standards Publication (FIPS) 200* directs that all Federal Government agencies ensure that adequate security controls be implemented for their Automated Information Systems (AIS). The guidelines provided in *FIPS 200* are applicable to all federal information systems other than those systems designated as national security systems as defined in *44 U.S.C., Section 35422*. It specifies that there are three types of security controls: Technical, Management, and Operational. The *USPTO IT Security Handbook* describes how USPTO will comply with these and other related directives.

Information Technology (IT) resources are invaluable to the United States Patent and Trademark Office (USPTO) and must be protected from loss, unauthorized alteration or access, and accidental disclosure. Since USPTO information promotes competitive, entrepreneurial business, this information must also be legally protected. IT security policy must be established, implemented, regularly reviewed and updated, and complied with for the protection of these critical resources.

The IT security policies captured in this document were developed to meet the minimum legally and federally mandated requirements for information security and are based on the Federal Government standards and procedures issued by OMB, NIST, and the General Services Administration (GSA). Appendix A provides a list of references used in developing this policy.

The unifying vision for the *USPTO IT Security Handbook* is based on having the following core program elements:

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- Security Planning, including defining and implementing security roles and responsibilities
- Capital Planning
- Security Awareness and Training
- Information Security Governance
- System Development Lifecycle
- Risk Management
- Certification & Accreditation, including certification testing
- Configuration Management
- Incident Response
- Performance Measures
- Security Products and Services Acquisition
- Contingency Planning

## **1.2 Policy**

This Handbook defines authorities and responsibilities necessary to establish an effective IT Security Program within the USPTO in order to help protect all USPTO information, applications, systems, networks, and IT infrastructure and resources from loss, misuse, and/or unauthorized modification, disclosure, or access. The IT security policies address specific requirements as set forth in federal laws and regulations, OMB Circulars, NIST special publications, and additional management, operational and technical controls addressing USPTO-specific IT Security concerns. IT security policy formulation and maintenance is the responsibility of the Information Technology Security Management Group (ITSMG).

## **1.3 Roles and Responsibilities**

All USPTO employees and contractor employees have IT security responsibilities. The USPTO IT Security Roles and Responsibilities are defined as follows:

### ***USPTO Chief Information Officer***

Within the USPTO, the role of Authorizing Official (AO) is assigned to the CIO. The CIO manages USPTO's IT infrastructure and risk management program. The CIO has the following IT Security responsibilities:

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- Develop, maintain, and oversee the USPTO IT Security Program
- Appoint, in writing, a Chief Information Security Officer to implement the IT Security Program within USPTO
- Ensure, in coordination with senior USPTO officials, the implementation of the requirements of a USPTO-wide IT Security Program (as specified in Section 3544, paragraph (b), of the FISMA)
- Ensure the USPTO annually performs an independent evaluation of the IT Security Program and its practices (as specified in Section 3545 of the FISMA)
- Provide overall management of and leadership and direction to the IT Security Program
- Assist and advise senior agency officials regarding their responsibilities for security, including system security plans
- Report regularly on the status of the IT Security Program to the Director and advise the Director on Security matters
- Consult with and briefs USPTO Executive Management regarding all critical information system security issues
- In coordination with other agency officials, report annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions
- Assess and advise the Director of weaknesses in the IT Security Program, as appropriate, for annual accountability reporting
- Ensure managers for all IT resources are identified and that Certification and Accreditation (C&A) for those resources are accomplished within the planned timeframe
- Determine the acceptable level of residual risk for an AIS and if an AIS will adequately protect sensitive USPTO information
- Approve System Security Plans
- Review the Security Accreditation Package (SAP) and sign the Accreditation Letter. In addition to granting an Authorization To Operate (ATO), , the CIO can issue a Deny Authorization to Operate (DATO) for an AIS (or halt operations if the system is already operational), if an unacceptable level of security risks exists
- Monitor and report IT Security Program compliance with Federal laws and USPTO IT security policies
- Serve as the IT Security liaison to external organizations

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- Ensure sufficient resources are available to implement the USPTO IT Security Program in coordination with the Director and the Heads of USPTO Business Units
- Ensure USPTO IT security planning and execution is practiced throughout the life cycle of each USPTO system
- Ensure a USPTO Computer Incident Response Team (CIRT) is staffed, trained, and maintained in a state of readiness
- Ensure that persons with IT security responsibilities have appropriate role-based training
- Assist oversight groups in compliance reviews and other reporting requirements
- Provide feedback to oversight groups on the status of the program in USPTO and suggest improvements or areas of concern in the USPTO program
- Establish an overall strategy for the IT Security Awareness and Training Program
- Ensure the program is sufficiently staffed and funded to achieve its approved objectives in a timely manner.
- Ensure the role-based training of USPTO personnel with significant security responsibilities
- Ensure effective tracking and reporting mechanisms are in place to accurately determine course completion, and to evaluate the awareness and training program
- Establish plans, procedures and schedules to correct any IT security awareness and training material weaknesses identified during formal inspections and evaluations
- Ensure that USPTO IT security policies are developed, approved, and maintained in a timely manner

### ***USPTO Business Area Heads***

USPTO business areas heads have assigned Authorizing Officials who co-sign with the CIO AO for those business systems under his/her area of responsibility. The following responsibilities apply to the USPTO Business Area Heads for Patents and Trademarks:

- Provide feedback to the Chief Information Security Officer (CISO) on the status of the program in the business area, as required by FISMA, and suggest improvements or address areas of concern in the business area security program or any other agency-wide security program or activity.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

***USPTO Chief Information Security Officer (CISO) / Senior Agency Information Security Officer (SAISO)***

At the USPTO, the CISO has certifying responsibilities. The CISO is the agency official responsible for: (i) carrying out the security executive under FISMA; (ii) possessing professional qualifications, including training and experience, required to administer the information security program functions; (iii) having information security duties as that official's primary duty; and, (iv) heading an office with the mission and resources to assist in ensuring agency compliance with FISMA. The CISO is responsible for determining the level of effort and resources required for AIS C&A; reviewing the AIS Security Categorization (SC); and, performing analysis and accepting the AIS SSP. The CISO (or supporting staff member) may also serve as the Authorizing Official's designated representative responsible for providing accreditation recommendations to the AO. The CISO serves as the CIO's primary liaison to the Agency's authorizing officials, System Owners, and Information System Security Officers. Additionally, the CISO has the following responsibilities for IT Security:

- Identify resource requirements, including funds, personnel, and contractors, needed to manage the USPTO IT Security Program
- Develop and maintain USPTO IT security policy, procedures, standards, and guidance consistent with Federal requirements and provide protection for the electronic information and information systems that support the operations and assets of the agency including those provided or managed by another agency or contractor
- Develop, document, and implement subordinate plans for providing adequate security for networks, facilities, and systems or groups of information systems
- Coordinate matters of physical security for IT resources with the USPTO Security Office
- Ensure that all systems have current and effective IT security plans that accurately reflect system status
- Ensure that appropriate security features are implemented in new systems and that they at least meet the minimum-security requirements defined in this Policy
- Ensure the security of an information system throughout its life cycle and that IT security is integrated in the USPTO strategic IT planning and enterprise architecture efforts
- Ensure periodic assessments of the risk and magnitude of harm are performed that could result from the unauthorized access, use, disclosure, or disruption of information and information systems that support the operations and assets of the Agency
- Ensure that an AO, SO, and Information System Security Officer (ISSO) have been appointed for each AIS within the USPTO and maintain up-to-date records of these assignments

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- Ensure that SSPs are properly prepared for all IT systems owned and operated by the USPTO
- Coordinate the development, review, and acceptance of SSPs with the SO, ISSO, and the Authorizing Official
- Review SSPs as submitted, making appropriate written comments that will be sent to the originator for corrective action
- Ensure ISSOs review and update all SSPs, at least annually, and incorporate changes or completed milestone actions
- Develop, document, and implement, no less than annually, periodic Certification Testing (CT) to assess the effectiveness of information security policies, procedures, and practices
- Coordinate the identification, implementation, and assessment of common security controls
- Establish a process to track remedial actions to mitigate risks in accordance with Plans of Action and Milestones (POA&M) to address any deficiencies in the information security policies, procedures, and practices of the Agency
- Review proposed system changes and act as approval authority for changes that impact system security
- Lead development, implementation, and enforcement of USPTO IT Security policies and procedures
- Manage and oversee internal and external reviews and inspections to ensure compliance with established policies and procedures
- Serve as the principal Point of Contact (POC) on IT security activities within USPTO
- Ensure appropriate IT Security Awareness Training (which does not include system-specific training for users) is provided, including tracking the number of employees and contractors completing training, and providing reports annually to OMB on training completed
- Advise the SO of security features and procedures for systems
- Ensure the OCIO Configuration Management (CM) process and SDLC is used to maintain IT Security documentation and alert the ITSMG when significant changes to a major application or general support system are proposed
- Identify and recommend management, operational, and technical control improvements to management

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- Ensure appropriate incident response capabilities
- Interface and coordinate with the Office of the Inspector General (OIG) on IT Security reviews and issues
- Assign each USPTO system a unique identification number that will identify the Agency and the specific system. The unique identification number will remain the same for the life of the system
- Ensure that IT systems are categorized, in conjunction with other staff, as either major applications or general support systems
- Maintain a tracking system for implementation of the required controls and accreditation status for all USPTO systems
- Ensure that all systems have effective, quality security documentation in place, including:
  - risk assessment reports (RAR),
  - current and effective IT security plans that accurately reflect system status,
  - annual system self-assessments,
  - current and tested contingency plans (CPs), and
  - current certification and accreditation
- Maintain the major application and general support system inventory tracking and provide updated inventories to oversight groups as required
- Provide information to systems administrators and others concerning risks and potential risks to systems
- Notify SOs and ISSOs of user infractions identified during routine compliance assessments and any required actions
- Advise the CIO and business area heads of technological IT security advances that can be used on an agency-wide scale and provide reduced costs for IT security efforts
- Report to the CIO and provide reports for forwarding to external entities such as OMB, Government Accountability Office (GAO), and Congress on IT Security Program status
- Ensure that USPTO sponsored awareness and training material is appropriate and timely for the intended audience
- Ensure that all users and managers have an effective way to provide feedback on the quality and quantity of IT Security awareness and training material and its presentation

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- Ensure that IT Security awareness and training material is reviewed periodically and updated when necessary

### ***USPTO Compliance Officer***

The Compliance Officer (CO) is responsible for managing the IT Security Program compliance to FISMA and OMB requirements. The security responsibilities include management of data calls to external agencies, tracking of Plan of Actions and Milestones (POA&M), internal security control reviews including penetration testing, Privacy Act assurance and adherence, Private Key Infrastructure policy and adherence, and compliance of USPTO IT Security policies and procedures through the use of independent verification and validation methods.

### ***Certification and Accreditation Program Manager***

The C&A Program Manager is responsible for managing the C&A process for all Master AIS. The C&A Program Manager plays an essential role in security and is, ideally, intimately aware of functional system requirements, and builds the business case for the acquisition of appropriate security solutions that help ensure mission accomplishment in the face of real-world threats. Additionally, the C&A Program Manager has the following IT Security responsibilities:

- Possess the knowledge and skills to appropriately incorporate IT security throughout a system's SDLC process to protect the business operations and information the system supports
- Work with the Systems Owners, ISSOs and CISO to meet shared IT security responsibilities
- Ensure system development and operations staff are knowledgeable of the C&A requirements and processes for their systems and are provided related training

### ***USPTO System Owner***

Within the USPTO, the Information System Owner (ISO) role is assigned to the SO. The SO has responsibility for the Master System, while the role of managing individual systems within the master system is typically assigned to the ISSO. The SO has the following responsibilities for IT Security:

- Obtain and manage the budget throughout the project's life cycle against a project manager's delivered, locked baseline
- Ensure the security of data and application software residing on the system
- Determine and implement an appropriate level of security commensurate with the system sensitivity level
- Prepare and conduct the preliminary risk assessment and retirement risk assessment for all assigned AIS

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- Perform risk assessments every three years or sooner if there is a major AIS modification, to re-evaluate sensitivity of the system, risks, and mitigation strategies
- Develop and maintain the IT SSP in coordination with the System Administrator, the ISSO, the CISO, and end users
- Take appropriate steps to update the risk assessment and to reduce or eliminate vulnerabilities after receiving the security assessment results from the certification agent
- Update the SSP whenever a significant change occurs and ensure re-accreditation as the system undergoes a significant change or at least annually
- Develop, maintain, and review the SAP including IT SSPs and CPs for all systems under their responsibility and submit the SAP to the authorizing official or their designated representative
- Ensure that IT security policies are implemented for their AIS
- Oversee the Certification Test when the system undergoes a major change and conducting annual self-assessments of the AIS
- Establish system-level POA&M and implement and monitor corrective actions to timely completion
- Ensure the AIS is deployed and operating according to the agreed-upon security requirements
- Decide who has access to the system and grant individuals the fewest privileges necessary for job performance, re-evaluate the access privileges at least annually, and revoke access in accordance with agency guidelines upon personnel transfer, termination, or change in duties
- Establish appropriate rules of behavior for all systems that apply to all personnel managing, administering, or having access to the IT system(s)
- Ensure systems' personnel are properly designated, monitored, and trained, including appointment in writing of an individual to serve as the System Development Lead (SDL), if appropriate
- Inform appropriate agency officials of the need to conduct a security C&A effort and ensure that appropriate resources are available for the effort
- Assist in the identification, implementation, and assessment of common security controls specific to their assigned AIS(s)
- Conduct Continuous Monitoring activities including configuration management, control testing, POA&M updates, and reporting status for their assigned AIS(s)

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- Ensure they have the knowledge and skills to appropriately incorporate IT security throughout their system's SDLC process to protect the business operations and information the system supports
- Work with the CIO and CISO to meet shared IT security responsibilities

### ***USPTO User Representative***

The User Representative (UR) represents the operational interests of the user community and serves as a liaison for that community throughout the AIS system development life cycle. Additionally, the UR has the following responsibilities for IT Security:

- Assist in the security C&A process, when needed, to ensure mission requirements are satisfied while meeting the security requirements and employing the security controls defined in the SSP
- Provide input in the creation of the AIS CP
- Assist in the development of the Interconnection Security Agreement, and memorandum of Understanding documents
- Assist the SO with the annual review of the SSP and ensuring documented data sensitivity values for the AIS accurately reflect the confidentiality, integrity, and availability of the data

### ***USPTO Information System Security Officer***

The Information System Security Officer (ISSO) is responsible for implementing the system-level controls and maintaining system documentation. The ISSO also serves as the principal advisor to the authorizing official, SO, and CISO on all matters involving the security of the information system. The USPTO ISSO has the following IT Security responsibilities:

- In coordination with the SO and UR, develops and updates information in the SSP, CP, and RA for each AIS for which he or she is responsible
- Assist in all phases of the C&A process for assigned AIS
- Advise the SO and PM on AIS security
- Coordinate with other designated personnel in preparing the SAP, participate in post-accreditation activities, and ensure the appropriate operation security practices are maintained for assigned AIS
- Update the appropriate C&A security documents accordingly with the vulnerability results
- Implement the system-level controls and maintain system documentation

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- Assist the CISO in the identification, implementation, and assessment of the common security controls
- Coordinate with the SO any changes to the system and assess the security impact of those changes
- Advise the SO regarding security considerations in applications systems procurement or development, implementation, operation and maintenance, and disposal activities (i.e., life cycle management)
- Assist in the determination of an appropriate level of security commensurate with the impact level
- Conduct preliminary risk assessments, in coordination with the CISO, for new systems to obtain data sensitivity values
- Participate in risk assessments to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies
- Perform annual self-assessments of security controls
- Maintain cooperative relationships with business partners and other interconnected systems
- Manage remediation activities in support of regular vulnerability scanning, formal, tri-annual C&A, and during regular SDLC-based security controls testing
- Conduct continuous monitoring: update IT SSP upon major changes to the system; oversee testing for vulnerabilities which may have been introduced by the major change, and coordinate with the CISO in obtaining AO acceptance of risk prior to deployment of the major change
- Review and approve the CTP and Certification Test Report (CTR)
- Ensure IT security requirements are specified, developed, implemented, and evaluated throughout the planning, design development, operation and maintenance of their systems
- Assist with design, implementation, and evaluation of awareness and training activities for the users, operators and maintainers of their systems
- Provide feedback on the effectiveness of training activities
- Collaborate and coordinate with the CISO to ensure the collective and interconnected USPTO IT environment is secure

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- Possess the knowledge and skills to appropriately incorporate IT security throughout their system's SDLC process to protect the business operations and information the system supports
- Ensure that all users of their systems are appropriately trained in, and know how to fulfill, their IT security responsibilities before allowing users access to their systems
- Work with the CIO and CISO to meet shared IT security responsibilities
- Notify the USPTO CIRT of any suspected incidents in a timely manner and assist in the investigation of incidents as necessary

### ***USPTO Certification Agent***

Within the USPTO, the Certification Agent (CA) has the role of Certifier. The CA is responsible for conducting a security certification, or comprehensive assessment of the management, operational, and technical security controls in an AIS to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The CA also provides recommended corrective actions to reduce or eliminate vulnerabilities in the information system and completes an independent assessment of the SSP to ensure the plan provides a set of security controls for the information system that is adequate to meet all applicable security requirements. The CA has the following additional IT Security responsibilities:

- Support the SO in accomplishing the C&A process
- Accept security responsibility for C&A activities
- Verify AIS users have proper and relevant security awareness and training
- Review the SAP and make recommendations to the AO
- Prepare accreditation letters for AIS and manages system technical, operational, and management controls to determine risk
- Assist in determining the acceptable residual risk level of the AIS
- Conduct comprehensive evaluation of the management, operational and technical controls in the IT system to determine: (a) the effectiveness of those controls in a particular operating environment; and, (b) the vulnerabilities in the system after the implementation of such controls
- Review the *Federal Information Processing Standards (FIPS) 199 Security Categorization, along with the user representative*, in an effort to determine if the impact to the security categories - confidentiality, integrity, and availability - is consistent with the USPTO mission

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- Review the SSP to determine if the vulnerabilities in the AIS are actually what the plan produces

### ***USPTO System and Network Administrators***

USPTO system and network administrators are responsible for certain aspects of system security, such as adding and deleting user accounts as authorized by the SO, as well as normal operations of the system in keeping with job requirements. The role of a System Administrator may include security of local area network (LAN) and application administration. System and network administrators shall:

- Assist in the development and maintenance of IT SSPs and CPs for all systems under their responsibility
- Participate in risk assessments to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies
- Participate in self-assessments of system safeguards and program elements and in C&A of the system
- Evaluate proposed technical security controls to assure proper integration with other system operations and the secure baseline configuration
- Identify requirements for resources needed to effectively implement technical security controls
- Develop system administration and operational procedures and manuals as directed by the SO
- Evaluate and develop procedures that assure proper integration of service continuity with other system operations
- Notify the responsible ISSO, the responsible CISO of any suspected incidents according to established agency guidelines, and assist in the investigation of incidents if necessary
- Read and understand all applicable use policies or other rules of behavior regarding use or abuse of USPTO IT resources
- Know the systems and components for which they are directly responsible (e.g., network equipment, servers, LAN, etc.) and the sensitivity of the data they handle and take appropriate measures to protect them
- Know and abide by all applicable DOC and USPTO policies and procedures

### ***USPTO Computer Incident Response Team***

The USPTO CIRT serves as a single point of contact for security issues and coordinates incident response activities. The USPTO CIRT has the following IT Security responsibilities:

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- Review and, as required, respond in a timely manner to e-mails sent to the group e-mail address “USPTO CIRT”
- Take appropriate action regarding official virus or hoax warnings
- Review the Enterprise Asset Management System (EAMS) problem reports daily
- Perform investigations of suspect USPTO policy violations
- Escalate or report security incidents, as warranted, to the United States Computer Emergency Readiness Team (US-CERT)
- Receive and monitor security alerts and advisories from the US-CERT and take appropriate action in response to alerts and advisories
- Perform network security monitoring

### ***USPTO Senior Official for Privacy***

The USPTO Senior Official for Privacy ensures that the service(s) or system(s) being procured or developed meet existing privacy policies regarding protection, dissemination (information sharing and exchange) and information disclosure. Additional responsibilities include:

- Provide guidance and direction for safeguarding agency-wide information and records, including electronic records (*Executive Order 13353, OMB Memorandum 05-08*)
- Ensures system of records notices are posted appropriately in accordance with the Privacy Act
- Determine and implement appropriate steps to protect personal information from unauthorized access, use, disclosure, modification, disruption, or destruction (*Executive Order 13353, OMB Memorandum 05-08*)
- Assure that technologies used to collect, store, use, and disclose identifiable information allow for continuous auditing for compliance with privacy policies and practices (*Consolidated Appropriations Act of 2005, PL 108-447*)
- Determine and maintain appropriate documentation, including records showing compliance with information privacy laws, regulations and policies (*Executive Order 13353, OMB Memorandum 05-08*)
- Identify and remedy any deficiencies or weaknesses, and mitigate risks from non-compliance (*Executive Order 13353, OMB Memorandum 05-08*)
- Assure that all employees and contractors receive appropriate training and education regarding information privacy laws, regulations, policies, and procedures governing the handling of personal information (*Executive Order 13353, OMB Memorandum 05-08*)

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

## **2 INFORMATION TECHNOLOGY SECURITY PROGRAM MANAGEMENT**

All USPTO information, applications, systems, networks, and IT infrastructure and resources must be protected from loss, misuse, and unauthorized modification, disclosure, or access. USPTO has developed and implemented a Security Program that ensures adequate protection for all information and IT systems that collect, process, transmit, store, and/or disseminate information. The IT Security Program includes adequate and appropriate levels of protection for all IT resources within the organization, including hardware, software, physical, and environmental facilities that support IT systems, telecommunications, administrative processes, personnel, and data.

Cost-effective security controls are chosen based on stakeholder assessment of the risk and potential impact should any USPTO assets or information be compromised. USPTO must implement management, operational and technical security controls to protect sensitive and critical assets.

USPTO recognizes the range of interpretation that complicates efficient compliance with this and other policies. Therefore, USPTO has implemented a three-tier model of policy, procedure, and guidance including:

1. Policy as identified in appendices AAO 212-4 and the USPTO IT Security Policy Management Policy;
2. Guidance as identified in IT Security Standards documents; and
3. Procedures as identified in Security Bulletins.

### **2.1 Purpose**

The United States Congress and the OMB have instituted a number of laws, regulations, and directives that govern establishment and implementation of federal information security practices. These laws, regulations, and directives establish federal and agency-level responsibilities for information security, define key information security roles and responsibilities, identify minimum information security controls, specify compliance reporting rules and procedures, and provide other essential requirements and guidance. These laws and regulations place responsibility and accountability for information security at all levels within federal agencies, from the agency head to IT users. They also provide an infrastructure for developing and promulgating detailed standards and implementation guidance to federal agencies and overseeing implementation of required practices through NIST and the GAO, respectively. At a minimum, information security in a federal department or agency must meet the requirements as they are detailed in applicable legislation, regulations, and directives. Agencies should tailor their information security policies and practices to their organization's own missions, operations, and needs.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

*OMB Circular A-130, FISMA Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources*, establishes a minimum set of controls to be included in federal automated information security programs, assigns federal agency responsibilities for the security of automated information, and links agency automated information security programs and agency management control systems.

### **2.1.1 Security Categorization (Sensitivity Rating Level)**

To establish sensitivity ratings and levels, the Security Categorization (SC) for each information type and AIS must be determined. The criteria for establishing security categories are defined in Federal Information Processing Standards 199, *Standards for Security Categorization of Federal Information and Information Systems*. Refer to *the Risk Assessment ITSS* for specific process guidance, since this process is designed to be accepted as part of the preliminary risk assessment for new major applications.

### **2.1.2 Security Objectives – Confidentiality/Integrity/Availability**

There are three security objectives defined by NIST as building blocks for the establishment of a complete list of agency security objectives - confidentiality, integrity, and availability. The objectives are used within the C&A process to determine the risks and impact of vulnerabilities within an AIS.

These objectives are defined as:

- **Confidentiality** - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information (*44 U.S.C., SEC. 3542*).
- **Integrity** - Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity (*44 U.S.C., SEC. 3542*).
- **Availability** - Ensuring timely and reliable access to and use of information (*44 U.S.C., SEC. 3542*).

#### **2.1.2.1 Confidentiality**

System and data confidentiality refers to the protection of personal privacy and proprietary information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

The USPTO manages information that has very specific rules governing its access and its privacy. Access to this information is restricted to those people who have a need to see or use it in performing their jobs. This is the concept of “need to know.” By limiting access in this way, only the minimum number of people necessary is granted access.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

Access to information is granted based on Privacy Act provisions, the nature of the specific request, and permission of the employee's supervisor with the knowledge and consent of the appropriate Head of USPTO Business Unit and Project Manager. All information, applications and systems have Heads of USPTO Business Units and the owners determine who will be allowed access and what permissions will be assigned to each user.

The System Owner shall ensure that sensitive data is identified in the SSP and shall identify and document appropriate management, operational, and technical controls in the SSP to protect the confidentiality of that data.

USPTO shall protect the most critical information during transmission by using *NIST FIPS 140-2* compliant encryption that makes the information unusable to someone who does not have the approval to use or see the information. These confidentiality services may be provided through the use of firewalls or other security techniques or products such as virtual private network (VPN) products.

### **2.1.2.2 Integrity**

System and data integrity refers to the requirement that information be protected from improper modification or destruction and ensuring information non-repudiation and authenticity. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. The violation of integrity may be the first step in a successful attack against system availability or confidentiality. For these reasons, loss of integrity reduces the assurance of an IT system.

The USPTO uses Access Controls (Refer to FIPS 200) to ensure that only authorized users are allowed to change information. System Owners limit the permissions of users to those necessary to do their job. During transmission, the same techniques that protect the confidentiality of USPTO information also protect its integrity.

SOs shall ensure that methods to protect the integrity of the systems and data are implemented and documented in the SSP and that appropriate management, operational, and technical controls are identified and documented in the SSP to help guarantee the integrity of systems and data.

### **2.1.2.3 Availability**

If a mission-critical system is unavailable to its end users, the organization's mission may be negatively affected. Loss of system functionality, for example, may result in loss of productive time, thus impeding customers' abilities to file or retrieve information and otherwise perform critical functions and operations.

SOs shall oversee efforts to ensure that systems availability and data methods and processes are implemented and documented in the SSP. They shall also identify and document appropriate management, operational, and technical controls in the SSP to help ensure the availability of systems and data.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

## **2.2 Policy Development and Maintenance**

IT security policies are developed by USPTO managers who have IT security responsibilities, with input from technical personnel who will be responsible for implementing the policies and resulting procedures. The highest-level security policies are contained in this Handbook, with policies relating to detailed procedures and operations contained in ITSS and Security Bulletins (SBs).

This AAO 212-4 and subsequent revisions are maintained by the OCIO and approved by all business area executives, including the Chief Financial Officer, General Counsel, Head of Patents, Head of Trademarks, Chief Administrative Officer, and CIO. The ITSMG has the overall responsibility of managing IT security policies at the USPTO. ITSS and (SBs) are also developed and maintained by the ITSMG.

IT Security policies shall be reviewed annually from the date of issuance by ITSMG or upon significant changes. Refer to the *IT Security Policy Management Policy* for further details.

### **2.2.1 IT Security Standards**

ITSS are developed and published on an as-needed basis and are partly designed to provide guidance for completing IT security artifacts incorporated into the USPTO SDLC. They contain USPTO-wide technical standards for the implementation and execution of various portions of the IT security program and policies. An ITSS is designed to aid the management and performance of tasks necessary to successfully produce an operational AIS. ITSSs include descriptions of the roles and responsibilities for performing the tasks, and standards for the associated work products. ITSSs shall be reviewed annually from the date of issuance by ITSMG or upon significant changes.

### **2.2.2 Security Bulletins**

Security Bulletins (SBs) are developed and published on an as-needed basis. They provide prompt IT security-related guidance on current or urgent topics that need to be communicated to USPTO employees. An example of a Security Bulletin would be an informational memorandum to employees that would describe recent social-engineering attempts against Federal agencies and provide advice on how to handle such attempts.

In the absence of any USPTO-specific policy, Federal laws and regulations, OMB Circulars NIST Standards and Guidelines and Department of Commerce IT security policy shall be used to implement management, operational, and technical controls within the USPTO. Where USPTO policies are found to be in contradiction to any mandatory requirements as set forth in those higher-authority requirements, the higher-authority requirements shall be used and deficiencies in USPTO policy shall be reported to the ITSMG for corrective action.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

### **2.2.3 Baseline System Security Requirements**

To ensure the overall protection of system resources and information, the USPTO has established minimum requirements that each system, which processes, stores, or transmits information, shall meet. These requirements include:

- Access to USPTO systems, data, and information shall be limited to only those users who have a “need to know.” The concept of “Least Privilege” should be followed when determining user access rights. This concept means that only the level of access necessary for an authorized user to perform their duties should be granted and nothing more.
- Systems shall provide for individual accountability and record security events and actions of each user as part of an audit capability, so users of the system may be held accountable for their actions within the system.
- All users and system processes shall have the least number of privileges for the least amount of time necessary to perform assigned tasks.
- Systems shall ensure that residual information is sanitized removed before any system or system resource is reused or discarded.
- All software development shall comply with the Secure Application Coding Development policy.<sup>1</sup>
- All systems shall be designed and implemented in a manner that allows the enforcement of USPTO security policies and sound computer security engineering principles such as the implementation of Application Program Interfaces (APIs) for making services available to multiple AIS.
- Systems shall provide all the functions and facilities necessary to support the authorized administrators in the management of the system security functions.
- Security planning and costs shall be integrated into each system and capital planning development life cycle processes.
- Systems shall provide for continuity of operations by preventing or minimizing the impacts of security incidents that may interfere with normal information processing and mission-critical operations.
- To the degree feasible, security-related tasks shall be assigned to several individuals to maintain separation of duties and ensure that no single individual has total control of the

---

<sup>1</sup> As of this writing, the Secure Application Coding Development Policy is still draft, however ITSMG strongly advocates adherence to this policy until such time this policy is fully approved.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

system's security mechanisms and, therefore, no one individual can compromise the system completely.

- Annual computer security awareness training and, as appropriate, periodic role-based training shall be conducted for all those involved in managing, operating, or using any USPTO information resources or systems.
- To the maximum extent possible, baseline security requirements and/or recommendations established by USPTO, NIST, Center for Internet Security (CIS) benchmarks and operating system and application vendors/manufacturers shall be implemented to ensure secure configurations of USPTO IT systems. Please refer to the Secure Baseline Policy.

These requirements are met through the implementation of management, operational, and technical controls on USPTO systems for the environments in which they operate.

The implementation of these requirements must be based on an assessment of risk and an overall cost-benefit analysis.

## **2.3 Program and Budgets**

IT Security expenditures are planned at two levels: the program level (non-system) and the system level. Expenditures at the program level include infrastructure protection and maintenance for all systems connected to the USPTO network (PTONet), including servers, firewalls, routers, switches, etc. Expenditures at the AIS level include C&A activities, correcting vulnerabilities, and enhancements to improve security protection.

OMB requires that USPTO track and reports the percentage of its budget that is devoted to IT security; this information is reported annually to OMB.

## **2.4 Security Performance Measures and Metrics**

It is critical that an information security performance measurement program is implemented to evaluate the effectiveness of technical and non-technical information security safeguards, support mandatory data collections required by OMB and the OIG, and enable the creation, analysis, and reporting of information security performance measures. In accordance with NIST guidelines, security audits are conducted by the USPTO to evaluate security controls and the IT security program. All documentation produced as a result of these audits is considered sensitive and must be controlled to ensure confidentiality and integrity.

## **2.5 Reporting**

The USPTO IT Security Program is required to be compliant with Federal and DOC requirements. Subject to CIO release, the ITSMG is responsible for initiating and coordinating reporting requirements to include the following:

- FISMA annual report

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- Annual and quarterly POA&M
- USPTO IT System Inventory

ITSMG also supports the CIO in analyzing and recommending weakness declarations as part of annual accountability reporting. The CIO recommends to the Director of the USPTO any material weakness found in USPTO systems during security audits. Only the Director is authorized to declare or relieve material weakness as recommended by the Management Council and in consultation with the CIO. The CIO must review compliance reports including IG findings, NIST Self-Assessments, C&A status, training results, and other elements of the IT Security Program in making this recommendation. FFMIA requires reporting on material weakness.

### **3 MANAGEMENT CONTROLS**

Management controls typically involve those safeguards and countermeasures employed by USPTO to manage the security of the AIS and the associated risk to USPTO's assets and operations. There are four (4) security control families within the management class of security controls.

- Planning
- System and Services Acquisition
- Risk Assessment
- Certification, Accreditation, and Security Assessments

#### **3.1 Planning**

##### **3.1.1 Purpose/Requirements**

This management control provides guidance with completing SSPs for the USPTO. Per *DOC Minimum Implementation Standards*, the USPTO is required to provide adequate security for the protection of AIS throughout the SDLC. The SSP documents the system security requirements for confidentiality, integrity, and availability and how they are met throughout the AIS lifecycle. The SSP also describes the security controls (management, operational, and technical) that are in place or planned for meeting those requirements. The SSP outlines how information and processing capabilities are protected from loss, misuse, unauthorized access, modification, or adverse security-related events.

*OMB Circular A-130, Management of Federal Information Resources, Appendix III*, requires a System Security Plan (SSP) for every AIS. As a result, an SSP is prepared for each USPTO system requiring C&A.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

The *USPTO IT Security Handbook* and referenced policy and process documents address each of the Planning controls as noted in Table 3-1.

**Table 3-1 Planning Controls<sup>2</sup>**

Planning Controls				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
PL-1	Security Planning Policy and Procedures	PL-1	PL-1	PL-1
PL-2	System Security Plan	PL-2	PL-2	PL-2
PL-3	System Security Plan Update	PL-3	PL-3	PL-3
PL-4	Rules of Behavior	PL-4	PL-4	PL-4
PL-5	Privacy Impact Assessment	PL-5	PL-5	PL-5
PL-6	Security-Related Activity Planning	Not Selected	PL-6	PL-6

### 3.1.2 Policy

#### 3.1.2.1 Security Planning

In accordance with *NIST SP 800-53, Rev1*, the USPTO shall develop, disseminate, and periodically review/update: (i) a formal documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.

The *Security Planning ITSS*<sup>3</sup> addresses each security control within the Planning security control family.

#### 3.1.2.2 System Security Plan

An SSP shall be prepared for all AIS (master and component) that require C&A.

---

<sup>2</sup> The format for these tables involves the NIST 800-53 control number starting on the far left column, then there is a column containing the control name. The control baselines indicate whether a control applies given the system's overall FIPS 199 data sensitivity rating. For example, a system with an overall data sensitivity of low would not be required to implement control PL-6.

<sup>3</sup> Currently, the *Security Planning ITSS* is still in draft state. Once it is approved and implemented, it will be posted as appropriate and a notification sent to all relevant divisions.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- The SSP documents the system security requirements for confidentiality, integrity and availability and how they are met throughout the life cycle of the AIS.
- The SSP documents data sensitivity values and data types.
- The SSP also describes the security controls (management, operational and technical) that are in place or planned for meeting those requirements.
- The SSP outlines how information and processing capabilities are protected from loss, misuse, unauthorized access, modification, or adverse security-related events.
- Documentation used or created during the C&A process, as well as documentation developed in previous C&A tasks should be included or referenced in the SSP. The documents include risk assessments, CPs, configuration management plans, and system interconnection agreement(s).

Refer to the *Security Planning ITSS* for specific guidance with creating an SSP and Appendices E, F, and G for SSP templates within the *Certification and Accreditation ITSS*. The SSP also includes, as references, other security-related documents for the AIS. These documents are to be drafted and included as part of the SSP.

### **3.1.2.3 System Security Plan Update**

The SSP is a living document that requires updates throughout the AIS's life cycle as new threats, risks, vulnerabilities, security requirements, and major enhancements occur. As part of the Initiation Phase of an AIS C&A, the SSP shall be updated. The purpose of this update is to (i) review the *FIPS 199* security categorization; (ii) analyze the SSP (including the System Boundary Definition); (iii) update the SSP; and (iv) obtain acceptance of the SSP by the AO and CISO prior to conducting an assessment of the security controls in the AIS. This is especially important with respect to the System Boundary Definition. The SSP shall be updated annually, or each time there is a change in the system that affects the system's security infrastructure or posture, design, and functionality. Examples of items that should be reviewed for change in the SSP include:

- System Owner
- Information System Security Officer
- Authorizing Official
- System Architecture
- System Status

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- System Interconnections
- System Scope
- C&A Status

**NOTE:** This is not an inclusive list of items that are to be reviewed in the SSP.

Refer to the *Security Planning* and *Certification and Accreditation ITSS* for specific policy and process guidance.

### **3.1.2.4 Rules of Behavior**

The USPTO shall establish and make readily available to all AIS users a set of rules that describes their responsibilities and expected behavior with regard to information and AIS usage. Content contained in the *Rules of Behavior* includes, but is not limited to:

1. Responsibilities, expected use of system, and behavior of all users
2. Appropriate limits on interconnections
3. Privacy and personally identifiable information
4. Peer to Peer Software Usage Restrictions
5. Service provisions and restoration priorities
6. Consequences of behavior not consistent with rules
7. Additional topics may include:
  - Remote Access – Work at home
  - Connection to the Internet
  - Use of copyrighted work
  - Unofficial use of government equipment
  - Assignment and limitations of system privileges and individual accountability
  - Password usage
  - Searching databases and divulging information.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

### **3.1.2.5 Privacy Impact Assessment**

A Privacy Impact Assessment (PIA) shall be conducted on AIS in accordance with *OMB Memorandum-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. As part of the USPTO System Development Life Cycle Process (SDLC), and in accordance with section 208 of the E-Government Act of 2002. Privacy Threshold Analysis (PTA) shall be conducted prior to the development or procurement of any IT system or for significant modification to an existing IT system. A Privacy Impact Assessment (PIA) shall be conducted if the results of the PTA indicate privacy information is present. The information captured during the PIA includes:

1. Type(s) of information that will be collected (nature and source)
2. Why the information is being collected
3. The intended use of the information
4. With whom the information will be shared
5. What opportunities individuals have to decline or consent to providing information and how individuals can consent
6. How the information will be secured
7. Whether a system of records is being created under the Privacy Act

A PIA template is included as a supporting appendix to an SSP. A PIA template is located as an appendix in the *Security Planning ITSS* and is also documented in the USPTO SDLC. Refer to the *IT Privacy Policy* for additional policy and procedures.

## **3.2 System and Services Acquisition**

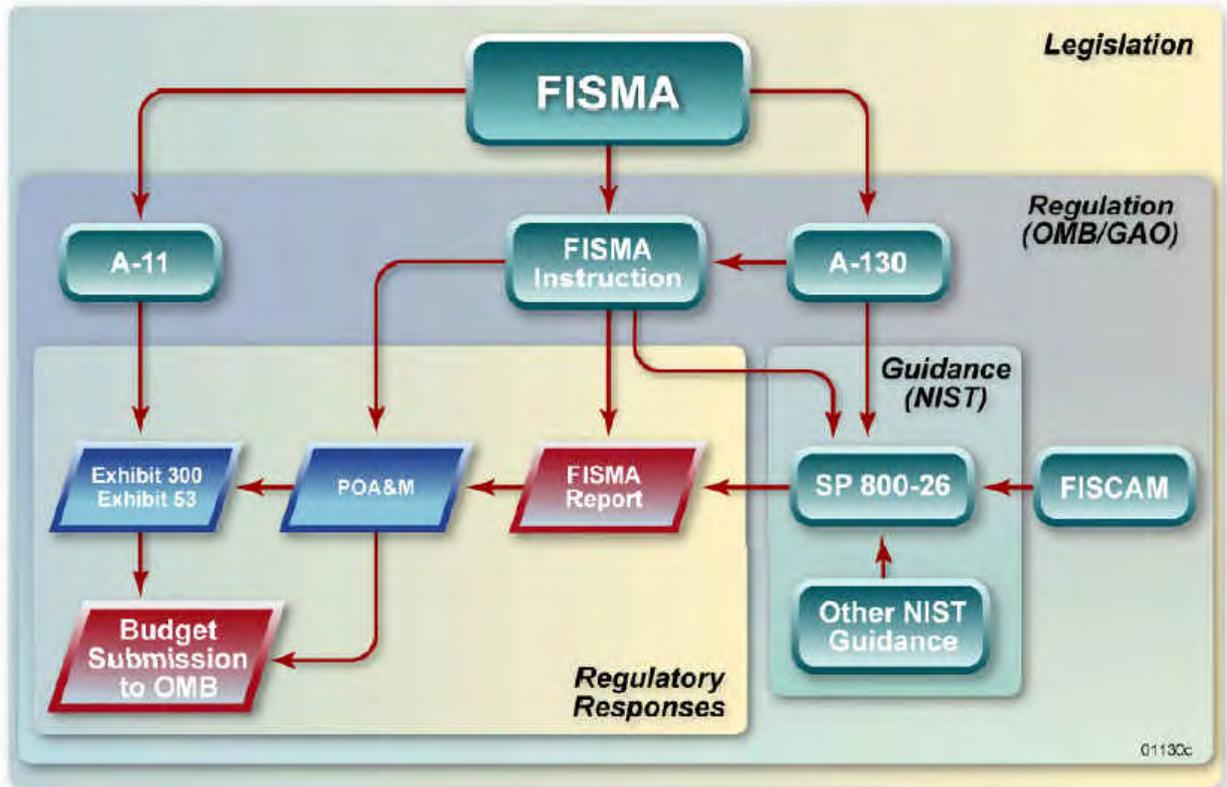
### **3.2.1 Purpose/Requirements**

This management control ensures that AIS are protected through planning for capital resources, incorporating an SDLC methodology that includes security considerations, planning for system acquisition/purchase which includes security requirements and specifications, employing software usage and installation restrictions, and ensuring that providers of AIS services protect information, applications, and services. This control applies to all employees and contractor employees unless otherwise stated.

*OMB Circular A-11, Preparation, Submission and Execution of the Budget, OMB Memorandum M-00-07, Incorporating and Funding Security in Information Systems Investments, and NIST Special Publication 800-65, Integrating IT Security into the Capital Planning and Capital*

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

*Investment Control Process*, provide specific guidance for agency security funding and capital planning. Figure 3-1 illustrates the process for securing funds in support of information security tasks.



**Figure 3-1: IT Security and Capital Planning Regulations and Guidance**

The *USPTO IT Security Handbook* and referenced policy and process documents address each of the System and Services Acquisition controls as noted in Table 3-2.

**Table 3-2: System and Services Acquisition Controls**

Systems and Services Acquisition Controls				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	SA-2	SA-2	SA-2
SA-3	Life Cycle Support	SA-3	SA-3	SA-3
SA-4	Acquisitions	SA-4	SA-4 (1)	SA-4 (1)
SA-5	Information System Documentation	SA-5	SA-5 (1)	SA-5 (1) (2)
SA-6	Software Usage Restrictions	SA-6	SA-6	SA-6
SA-7	User Installed Software	SA-7	SA-7	SA-7
SA-8	Security Engineering Principles	Not Selected	SA-8	SA-8
SA-9	External Information System Services	SA-9	SA-9	SA-9

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

Systems and Services Acquisition Controls				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
SA-11	Developer Security Testing	Not Selected	SA-11	SA-11

### 3.2.2 Policy

#### 3.2.2.1 System and Services Acquisition

In accordance with *NIST SP 800-53, Rev1*, the USPTO shall develop, disseminate, and review (i) a formal, documented, system and services acquisition policy that includes information security considerations and addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and, (ii) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

#### 3.2.2.2 Allocation of Resources

The USPTO shall determine, document, and allocate, as part of its capital planning and investment control process, the resources required to adequately protect all AIS. The SDLC requires consideration of IT security in budget requests. As a result, business areas shall include the capital asset budget planning process and follow a methodology consistent with *NIST SP 800-65*. *OMB Circular A-11* and Memorandum *M-00-07* require that security be built into and funded as part of the system architecture. As a result, each business area CIO is responsible for security roles as part of the IT investments and capital programming processes. The funding shall include all products, procedures, and personnel (Federal employees and contractors) that are primarily dedicated to or used for provision of IT security for the specific IT investment. Accordingly, investments in the development of new or the continued operation of existing AIS, both general support systems and major applications proposed for funding in the President's budget shall:

- Be tied to the DOC IT architecture;
- Be well-planned;
- Manage risk;
- Protect privacy and confidentiality; and
- Account for departures from NIST guidance.

#### 3.2.2.3 Life Cycle Management

IT Security is managed throughout a system's life cycle. This responsibility shall be assigned to the SO. System security is most effective when it is designed, developed, and integrated into a system as part of the development process.

This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.

The formal life cycle process follows the *USPTO System Development Life Cycle Process*. Security Controls are a critical part of the SDLC process, as they provide safeguards within the AIS designed to ensure security commensurate with the system's sensitivity level. Security Controls are critical for the execution of CTs, Risk Assessments, and drafting a new or refining an existing SSP.

In Figure 3-2, the USPTO SDLC is mapped to the NIST Information System Development Life Cycle.

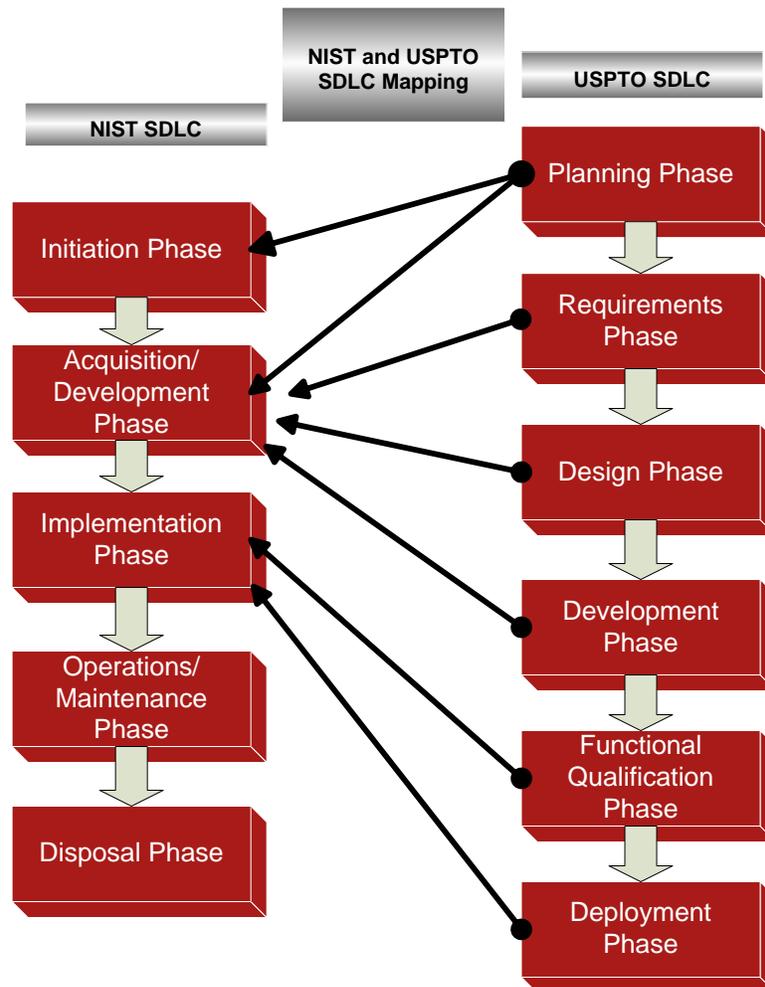


Figure 3-2: NIST and USPTO SDLC Mapping

IT Security products shall be developed and updated during each phase of the USPTO SDLC. The *Certification and Accreditation ITSS* identifies IT security activities and documentation required during each phase of a system's life cycle.

### 3.2.2.4 Acquisitions

The USPTO shall include security requirements and/or security specifications, either explicitly or by reference, in AIS acquisition contracts, based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards. Funding

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

shall be identified for AIS technologies, programs and methods used to determine information security costs for all division systems. The FAR must be complied with.

As part of the acquisition process, the following requirements and guidance shall be given to providers of external information system services:

- The contractor shall implement adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance;
- Establish service level agreements; and
- Monitor security control compliance.

For all contracts and solicitations that contain Information Technology services, there are two security clauses that shall be included:

- Commerce Acquisition Regulation (CAR) 1352.239-73 “*Security Requirements for Information Technology Resources*” (October 2003)
- CAR 1352.239-74 “*Security Processing Requirements for Contractors/Subcontractors Personnel for Accessing USPTO Automated Information Systems*”

For all contracts and solicitation that contain services that require contractor access to a system that processes privileged access to USPTO data, the following security clause shall be included:

- CAM 1337.70, “*Security Processing Requirements for Service Contract*”

These clauses can be found in the *PM 2006-06 Information Security in Acquisitions.pdf* document and the *CAM 1337.70 Personnel Security Processing.pdf* document which are located on the DOC intranet.

The DOC Office of Acquisition has developed a flowchart (see Figure 3-3) that can be used as guidance to assist contracting professionals with making key information security decisions as part of the acquisition process.

This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.

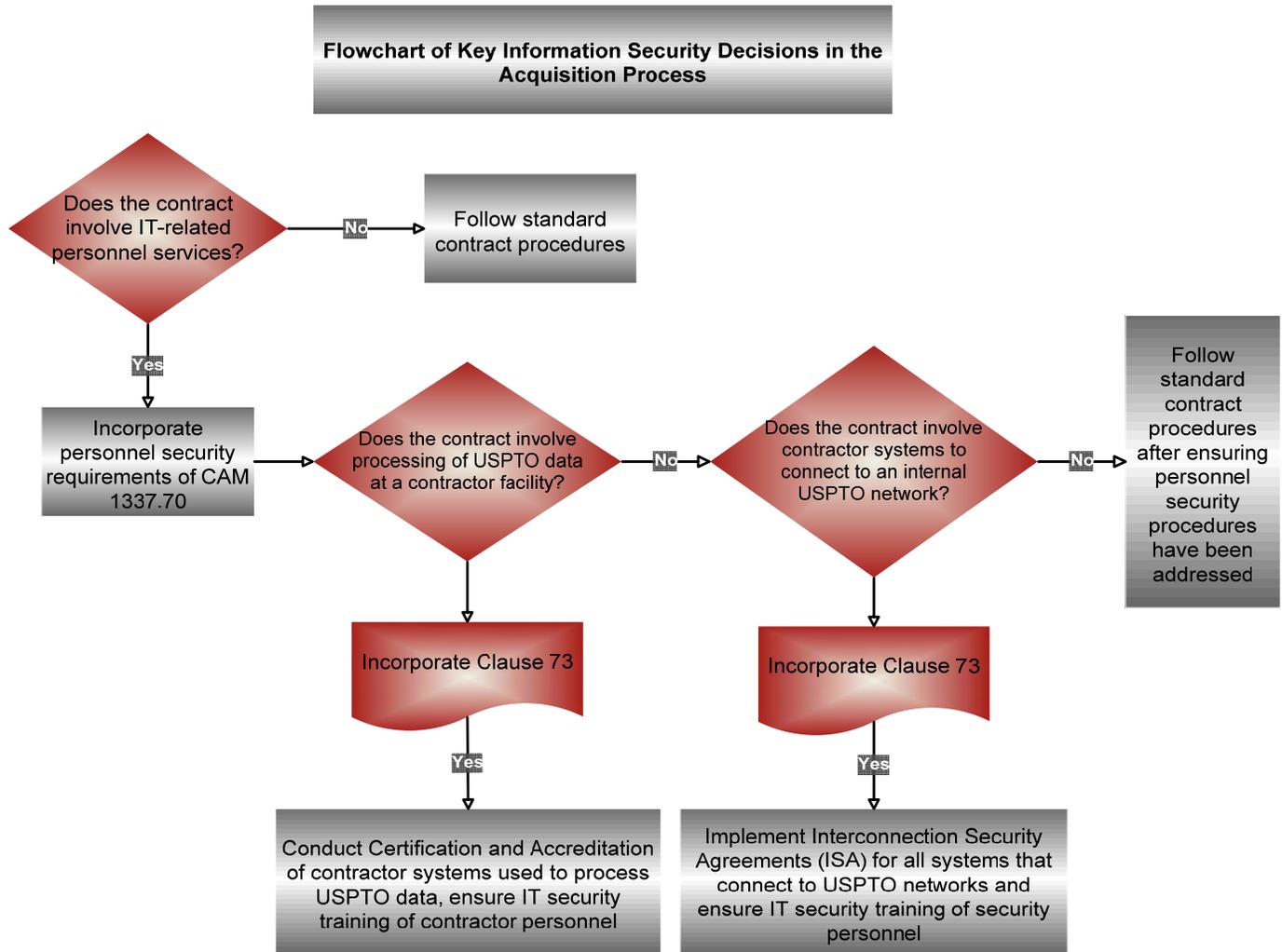


Figure 3-3: Flowchart of Key Information Security Decisions in the Acquisition Process

The following seven-step methodology developed within *NIST SP 800-65* and illustrated in Figure 3-4 can be used as guidance to establish high-priority corrective actions for immediate funding:

1. **Identify the Baseline:** Use information security metrics or other available data to baseline the current security posture.
2. **Identify Prioritization Requirements:** Evaluate security posture against legislative and CIO-articulated requirements and Agency mission.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

3. **Conduct Enterprise-Level Prioritization:** Prioritize potential enterprise-level IT security investments against mission and financial impact of implementing appropriate security controls.

4. **Conduct System-Level Prioritization:** Prioritize potential system-level corrective actions against system category and corrective action impact.

5. **Develop Supporting Materials:** For enterprise-level investments, develop concept paper, business case analysis, and Exhibit 300. For system-level investments, adjust Exhibit 300 to request additional funding to mitigate prioritized weaknesses.

6. **Implement ITIRB and Portfolio Management:** Prioritize agency-wide business cases against requirements and CIO priorities and determine investment portfolio.

7. **Submit Exhibit 300s, Exhibit 53, and Conduct Program Management:** Ensure approved 300s become part of the agency's Exhibit 53; ensure investments are managed through their life cycle (using Earned Value Management [EVM] for Development/Modernization/Enhancement investments and operational assessments for steady state investments) and through the GAO's Information Technology Investment Management (ITIM) maturity framework.



**Figure 3-4: IT Security and Capital Planning**

### 3.2.2.5 System Documentation

Adequate documentation shall be available, protected, and distributed for all AIS. AIS documentation includes descriptions of the hardware and software as well as policies, standards and procedures related to system security. The AIS sensitivity level shall identify what specific documentation is required in accordance with the following SA-5 control enhancements:

- Moderate- and high-sensitivity systems shall include documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the AIS, with sufficient detail to permit analysis and testing of the controls.
- High sensitivity systems shall include documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the AIS, with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

Table 3-3: describes the IT Security documentation required for all (Low/Moderate/High) AIS and who is responsible for each document.

**Table 3-3: Required System Security Documentation**

<b>Required System IT Security Documentation</b>	
<b>Document</b>	<b>Responsibility</b>
E-Authentication Risk Assessment (if applicable)	ISSO
Risk Assessment Report	System Owner
System Security Plan	System Owner
Certification Test Plan	ISSO
Certification Test Report	ISSO
Contingency Plan	System Owner
Configuration Management Plan	System Owner
IT Security Self-Assessment	System Owner
Interconnection Security Agreement(s) (as applicable)	System Owner
Plan of Action and Milestones	System Owner
Memorandum of Understanding (as applicable)	System Owner
Rules of Engagement	ISSO
Scan Authorization Letter	ISSO
Certification Recommendation	IT Security Officer
Accreditation Letter (ATO/IATO/DATO)	AO
AIS Security Status Report(s)	System Owner

All documentation shall be reviewed and updated annually, or whenever there are significant changes affecting the security of the system. A significant change is defined by the System Owner through the use of the *Security Controls Assessment Determination* form. Examples of significant changes include, but are not limited to:

- Upgrades/modifications to the operating system;
- Installation/upgrade/change to a server; and
- Additions or modifications to system ports, protocols, or services.

IT Security documentation shall be under CM Control in the OCIO’s CM System.

### **3.2.2.6 Software Usage Restrictions**

Established software usage requirements and guidance shall apply to all employees and contractor employees who use information resources. These requirements include:

- All software loaded on information systems must have authorized licensing agreements.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- Unauthorized Peer-to-Peer file/software sharing technology is not permitted. A policy specifically for Peer-to-Peer file sharing is currently available in draft form.
- Software monitoring applications are used to ensure that all software deployed on information resources adheres with federal laws and vendor contractual license agreements.

### **3.2.2.7 User Installed Software**

Explicit rules governing the installation of software on information resources by employees shall be enforced. Your rights under the limited personal use policy do not authorize installation of software.

The following software downloads are prohibited:

- Software related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities, or for the sole purpose of personal use;
- Downloading of Computer video games;
- The creation, download, viewing, storage, copying, or transmission of pornographic, sexually explicit, or sexually oriented materials unless expressly permitted by supervisor for execution of the business mission; and
- Unauthorized computer software that includes privacy information, patent, copyright, trademark, or material with other intellectual property rights, proprietary data, or export controlled software.

**Note:** For employees or contractor employees who have a need to download software from restricted sites (as part of their job function), an exemption shall be submitted and approved in writing by a supervisor. The supervisor shall provide a list to the CISO of those employees who have been authorized to download software from restricted sites. All requests for user installed software should follow the *Software Product Approval Process*. Only approved USPTO software shall be considered for installation. The software must be **tested** to ensure system compatibility with USPTO configuration baselines before being loaded on any information resources. Refer to the *Software Product Decision Document* for specific process guidance.

**NOTE:** USPTO contractor facilities shall satisfy this requirement based on industry best practice and contractor policy and process specific to the *NIST SP 800-53, Rev.1, User Installed Software (SA-7) Security Control*. Contractors should also consult with USPTO staff on compliance requirements.

### **3.2.2.8 Security Engineering Principles**

In accordance with *NIST SP 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Rev. A*, each new and modified AIS shall be designed and implemented using security engineering principles as part of the SDLC. For legacy

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

systems, the security engineering principles shall be applied to system upgrades and modifications as applicable based on the current state.

### **3.2.2.9 External Information System Services**

Providers of external information system services shall be required to 1) employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements, and, b) monitor security control compliance. External services are those implemented outside of the system accreditation boundary.

### **3.2.2.10 Developer Security Testing**

Security controls shall be tested as part of the SDLC. Among the required security artifacts are a *Security Controls Assessment Plan*, and a *Security Controls Assessment Report*. Developmental security test results may be used in support of the security C&A process for the delivered AIS. Refer to the *Certification and Accreditation ITSS* and the *Certification Testing ITSS* for a detailed process overview.

## **3.3 Risk Assessment**

### **3.3.1 Purpose/Requirements**

This management control ensures that USPTO protects AIS by periodically assessing the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational AIS and the associated processing, storage, or transmission of organizational information.

Risk Management is the total process of identifying, controlling, and eliminating or reducing risks that conceivably affect system resources. It includes:

- Risk analysis (identification and analysis of the risks posed by threats to the system)
- Determination of appropriate protection levels for the resources
- Management decisions to implement selected security safeguards based on the risk analysis, including accepting residual risk, if necessary
- Effectiveness reviews

Risk Management encompasses two processes: Risk Assessment (RA) and Risk Mitigation (RM). These processes are described in *NIST SP 800-30, Risk Management Guide for Information Technology Systems*. Risk Management is the process that allows USPTO managers to balance the operational and economical costs of protective measures with the gains in mission capability that result from the protection of IT systems and data that support USPTO's mission(s).

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

*NIST SP 800-30* defines Risk Mitigation as the least-cost approach that implements the most appropriate controls to decrease mission risk to an acceptable level with minimal adverse impact on the organization’s resources and mission.

The loss of data and AIS information from natural and man-made threats can be as devastating and costly to USPTO as technical threats. As a result, the RA process considers technical as well as managerial and operational components.

The *Risk Assessment ITSS* addresses each RA security control as noted in Table 3-4.

**Table 3-4: Risk Assessment Controls**

Risk Assessment				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
RA-1	Risk Assessment Policy and Procedures	RA-1	RA-1	RA-1
RA-2	Security Categorization	RA-2	RA-2	RA-2
RA-3	Risk Assessment	RA-3	RA-3	RA-3
RA-4	Risk Assessment Update	RA-4	RA-4	RA-4
RA-5	Vulnerability Scanning	Not Applicable	RA-5	RA-5(1)(2)

### 3.3.2 Policy

#### 3.3.2.1 Risk Assessment

In accordance with *NIST SP 800-53, Rev 1*, the USPTO shall develop, disseminate, and periodically review/update: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

The RA process is integrated within the SDLC and shall be tailored to the particular phase of the USPTO SDLC in which it occurs. Some RA activities may not take place in all phases of the SDLC, or may take on a modified methodology. When assessing a system, provisions should be made for those security activities that may be missing. Part of the assessment will be determining which, or how many, activities need to be completed from prior phases in the SDLC. With respect to RAs completed by USPTO personnel, phases entered for purposes of RA are Initiation, Acquisition/Development, Operations/Maintenance, and Disposal. The approach used for RAs is described in the *Risk Assessment ITSS*.

#### 3.3.2.2 Security Categorization

To establish sensitivity ratings, the Security Categorization (SC) for each information type and the SC for the AIS shall be determined. The criteria for establishing security categories are

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

defined in *NIST SP 800-60, Guide for Types of Information and Information Systems to Security Categories, Volume I, and Volume II*. The *FIPS 199, Standards for Security Categorization of Federal Information and Information Systems*, provides criteria to determine the potential impact level for each security objective. Establishing a SC requires determining the potential impact for each security objective associated with an information type. Once the *NIST SP 800-60* sensitivity ratings have been established for each information type, the information is used to determine the SC for the system. An initial Preliminary Risk Assessment (PRA) -- documented in the USPTO SDLC -- provides the foundation for the SSP, including the establishment of an AIS sensitivity level by identification of Security Categories for the information system and information type, identification of threats to the AIS, determination of information and system sensitivity levels (*FIPS 199*), and validation of security controls necessary (*NIST SP 800-53, Rev. I*) to ensure AIS security. (System Owner and User Rep responsibility for input) Refer to the *Risk Assessment ITSS* for specific process guidance.

### **3.3.2.3 Risk Assessment Reports**

Assessments shall be conducted of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency (including information and AIS managed/operated by external parties). The Risk Assessment (RA) is a critical part of the SDLC process in accordance with *NIST SP 800-64, Security Considerations in the Information System Development Life Cycle*, as well as during tri-annual C&A execution. The RA determines whether the approved safeguards and security controls required to protect the system's assets are effective. An RA helps the staff determine appropriate controls commensurate with the system's required level of protection. The results are also used for refining the SSP.

The RA is updated whenever there are significant changes to the AIS or the facilities where the system resides or other conditions occur that may impact the security or accreditation status of the system. Refer to the *Risk Assessment* and *Security Planning ITSS* for specific process guidance.

Another kind of risk assessment is the E-Authentication Risk Assessment, which is part of the E-Gov initiative and is now required for FISMA reporting. The E-Authentication Risk Assessment requirement includes all applications and systems that are outward facing and web based.

### **3.3.2.4 Vulnerability Scanning**

Vulnerability scanning shall be performed at least quarterly for each moderate- and high-sensitivity AIS or when significant new vulnerabilities potentially affecting the system are identified and reported. Technical security controls are tested using Technical Vulnerability Assessments (TVAs). TVAs include automated scans and reviews of software configuration settings to test the operation of the system and application software technical controls. The TVA determines if the risk to confidentiality, integrity, availability, and accountability from internal and external threat sources from known vulnerabilities is being maintained at an acceptable level and that secure configuration policies are maintained. *NIST SP 800-42, Guideline on Network*

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

*Security Testing* identifies a number of automated tools that can be used to test technical controls. The selection of specific tools to be used is dependent on system requirements, scope of the project, operating system, configuration of the networking environment, and methods and tools used by hackers. The DOC recommends the use of multiple tools to confirm the results and ensure no vulnerabilities are overlooked. Refer to the *Risk Assessment* and *Certification Testing ITSS* for specific process guidance.

### **3.4 Certification, Accreditation, and Security Assessments**

#### **3.4.1 Purpose/Requirements**

This management control ensures that USPTO AIS have a level of system security in place that reasonably protects USPTO's information and/or processing capabilities.

Required by *FISMA*, security accreditation provides a quality review to implement security controls that effectively protect an IT system given mission requirements as well as technical, operational, and cost/schedule constraints. The C&A process consists of all tasks and documentation that contributes to and results in the C&A of an IT system.

The C&A process begins during the Planning Phase of a new system, continues during all remaining SDLC phases, and terminates upon the retirement of the system. Certification and Accreditation processes are defined as follows:

- Certification is the formal evaluation and testing of the security safeguards implemented in a computer system to determine whether they meet applicable requirements and specifications.
- Accreditation is the formal authorization by management for system operation, including an explicit acceptance of residual risks.

C&A is a "process," not an "event." The C&A of a system is not an end in itself, but rather represents a snapshot of the security posture of the system at that time. The validity of the accreditation will remain meaningful only if the plan and policy execution and enforcement is strictly adhered to, and assigned personnel fulfill their responsibilities.

The C&A process for AIS are required as per the following federal laws and regulations and DOC policy:

- *E-Government Act (Public Law 107-347), Title III - Federal Information Security Reform Act 2002 (FISMA), December 2002*
- *OMB Circular A-130, Appendix-III, Security of Federal Automated Information Resources*
- *Annual OMB Memoranda U.S. Department of Commerce, IT Security Program Policy and Minimum Implementation Standards*

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

Major applications are grouped into master systems to facilitate the C&A process. Consistent with the grouping of major systems and individual component systems into master systems described above, master C&A system boundary definitions are documented to describe the security boundaries for all C&A activities. Master C&A system boundary definitions are based on the business area requirements they support, dependencies of related interconnected systems, and management/budgetary authority that governs their use.

The *Certification and Accreditation ITSS* addresses these requirements and covers all Certification, Accreditation, and Security Assessments controls as noted in Table 3-5:

**Table 3-5: Certification and Accreditation Controls**

C&A Controls				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	CA-1	CA-1	CA-1
CA-2	Security Assessments	CA-2	CA-2	CA-2
CA-3	Information Systems Connections	CA-3	CA-3	CA-3
CA-4	Security Certification	CA-4	CA-4	CA-4
CA-5	Plan of Action and Milestones	CA-5	CA-5	CA-5
CA-6	Security Accreditation	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	CA-7	CA-7	CA-7

### 3.4.2 Policy

#### 3.4.2.1 Certification, Accreditation, and Security Assessment

In accordance with *NIST SP 800-53, Rev 1*, the USPTO shall: (i) periodically assess the security controls in organizational AIS to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational AIS; (iii) authorize the operation of organizational AIS and any associated AIS connections; and (iv) monitor AIS security controls on an ongoing basis to ensure the continued effectiveness of the controls.

#### 3.4.2.2 Certification Testing

Certification Testing (CT) is used to examine the effectiveness of system security controls with the objective of determining the true risk, or exposure, of the system to certain threats. The Certification Testing process is designed to determine and document whether AIS satisfy established security requirements through the development and execution of a Security Controls Assessment Plan (SCAP). The Security Controls Assessment Report (SCAR) presents the results of security test cases, which are used to test the security control features, implemented or planned, for master or component AIS. The CTR serves as the primary input to the RA, which

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

determines the threats, impacts and overall risks of the vulnerabilities. CT shall be conducted on each AIS to be certified and accredited.

The CT process consists of four phases:

- **Phase I: Identify AIS Security Requirements and Boundaries** – Security requirements are identified in order to verify that existing controls are in place and adequately protect the AIS. As part of this CT process, it is important to determine the techniques and frequency of testing to be conducted.
- **Phase II: Create a Security Controls Assessment Plan** –The SCAP includes the security requirements and assessment procedures for each AIS component, as identified and verified in the SSP boundaries, and complete test procedures for all security controls (technical, operational, management).
- **Phase III: Conduct Certification Testing and Document Results** – Activities associated with conducting AIS testing and documentation include: (i) preparing the AIS for testing; (ii) executing test procedures; (iii) recording results; and (iv) creating the draft SCAR.
- **Phase IV: Submit Certification Test Report** – A finalized SCAR is submitted to the AO, CISO, and ISSO for review and approval. Upon approval of the CTR, the SO prepares a POA&M document to track corrective actions necessary to mitigate identified vulnerabilities and reduce risk to a level acceptable to the Authorizing Official.

In addition to performing CT activities in support of new and existing AIS with major modifications, the USPTO shall perform self-assessments of AIS. The DOC requires all operating units to complete annual reviews, or self-assessments, of each AIS (See the *U.S. Department of Commerce, IT Security Program Policy and Minimum Implementation Standards*). A Self-Assessment conducted on a master system is used to measure security assurance. An RA is usually conducted in conjunction with or prior to a self-assessment.

The *Certification Testing ITSS* describes the assessment process, test requirements for both AIS under development and recertification, and development of plans and test procedures. It also provides the SCAP and SCAR templates.

### **3.4.2.3 System Interconnection/Information Sharing**

USPTO shall adhere to the *NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems* guidance for systems that connect to organizations external to the USPTO network boundary, which includes requirements for establishing Interconnection Security Agreements (ISAs). For those systems within the USPTO network boundary, ISAs are not required, as assessments of risk will have already been completed for all USPTO AIS.

The ISA specifies the technical and security requirements of the interconnection. There are four phases involved with establishing an interconnection;

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

1. **Planning** – All impacted organizations examine technical, security, and administrative issues and agree on the management and operation of the interconnection.
2. **Establishing** – All impacted organizations create and conduct a plan for establishing the interconnection.
3. **Maintaining** – All impacted organizations maintain the interconnection to ensure that the AIS is secure and operating properly.
4. **Disconnecting** – All impacted organizations may terminate the interconnection.

**NOTE:** The establishment of an interconnection may constitute a major change to an AIS, which requires re-certification and re-accreditation determination. The ISA is to be documented in the Certification & Accreditation package. Refer to the *Certification and Accreditation ITSS* for specific process guidance and an ISA template.

#### **3.4.2.4 Security Certification**

Security Certification is the second phase of the C&A process and consists of two major tasks: (i) security control assessment; and (ii) security certification documentation. Security Certification shall be conducted in support of the *OMB Circular A-130, Appendix III* and NIST SP 800-37 requirements for accrediting an AIS. The purpose of this phase is to determine if the security controls are correctly implemented, operating as intended, and produce the required outcome. This phase also addresses remedial actions planned to correct AIS security control deficiencies in order to reduce or eliminate vulnerabilities in the AIS. For moderate- and high-sensitivity AIS, an independent certification agent is employed to conduct an assessment of the security controls. Refer to the *Certification and Accreditation ITSS* for specific process guidance.

#### **3.4.2.5 Plan of Action and Milestones**

The POA&M shall document AIS vulnerabilities identified as a result of CTs, security impact analysis, and continuous monitoring activities. The POA&M document identifies activities, either planned or implemented, to correct security control issues or eliminate vulnerabilities in the AIS. The POA&M describes tasks that are required to facilitate these activities, resources required to accomplish the tasks, task milestones, and completion dates. The POA&M is an important document that shall be included in the C&A SAP. Refer to the *Certification and Accreditation ITSS* for specific process guidance and a POA&M template.

#### **3.4.2.6 Security Accreditation**

Security Accreditation is the third phase of the C&A process, consisting of two major tasks: security accreditation decision and security accreditation documentation. In this phase, the AO shall review and evaluate the SAP and determine if the residual risk is acceptable for the AIS. Refer to the *Certification and Accreditation ITSS* for specific process guidance.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

### **3.4.2.7 Continuous Monitoring**

Continuous Monitoring is the fourth phase of the C&A process. This phase consists of three major tasks: (i) configuration management and control; (ii) security control monitoring; and (iii) status reporting and documentation. In this phase, the SO shall be responsible for maintaining an acceptable level of risk, performing required FISMA activities, and ensuring that the AIS undergoes re-certification/re-accreditation when a major modification has occurred, or at least every three (3) years. The Continuous Monitoring process begins during the Operational phase for a new AIS and ends upon master or component AIS disposal. The Continuous Monitoring process is a joint activity between the business area and the OCIO.

Refer to the *Security Controls Assessment Determination Form* located in the *Certification Testing ITSS* to determine what criteria constitute a major system change. Refer to the *Continuous Monitoring*<sup>4</sup> and *Certification and Accreditation ITSS* for a complete overview of the Continuous Monitoring phase.

---

<sup>4</sup> Currently the *Continuous Monitoring ITSS* is under development. Once it is developed and implemented, a notification will be sent to all relevant divisions.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

## **4 OPERATIONAL CONTROLS**

Operational controls are those safeguards and countermeasures employed by an organization to support the management and technical security controls in the AIS. In contrast to technical controls that are primarily executed by the AIS, operational controls are typically executed by roles that support the system. There are nine (9) families within the operational class of security controls.

- Personnel Security
- Awareness and Training
- Physical and Environmental Protection
- Incident Response
- Media Protection
- System and Information Integrity
- Maintenance
- Contingency Planning
- Configuration Management

### **4.1 Personnel Security**

#### **4.1.1 Purpose/Requirements**

This Operational Control ensures that (i) individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) organizational information and AIS are protected during and after personnel actions such as terminations and transfers; and (iii) formal sanctions are invoked for personnel failing to comply with organizational security policies and procedures.

The *USPTO IT Security Handbook* and referenced policy and process documents address each of the Personnel Security controls as noted in Table 4-1:

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

**Table 4-1: Personnel Security Controls**

<b>Personnel Security Controls</b>				
<b>Control Number</b>	<b>Control Name</b>	<b>Control Baselines</b>		
		<b>Low</b>	<b>Moderate</b>	<b>High</b>
PS-1	Personnel Security Policy and Procedures	PS-1	PS-1	PS-1
PS-2	Position Categorization	PS-2	PS-2	PS-2
PS-3	Personnel Screening	PS-3	PS-3	PS-3
PS-4	Personnel Termination	PS-4	PS-4	PS-4
PS-5	Personnel Transfer	PS-5	PS-5	PS-5
PS-6	Access Agreements	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	PS-8	PS-8	PS-8

## **4.1.2 Policy**

### **4.1.2.1 Personnel Security**

In accordance with *NIST 800-53, Rev1*, the USPTO shall develop, disseminate, and periodically review/update: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

All personnel with responsibilities for the management, operation, maintenance, or use of computer resources and sensitive information shall have the required, appropriate management approvals and security clearances.

- Business Unit AOs shall authorize, in writing, any non-USPTO personnel who use Business Unit systems.
- Technical support personnel from outside USPTO, who perform maintenance on USPTO systems within USPTO-controlled facilities, shall be escorted at all times, unless they have been approved for unescorted access.
- USPTO-CIRT shall suspend access to USPTO systems upon credible perception of security threat or notice by appropriate authority (Office of Human Resources [OHR], supervisor).
- USPTO contracts shall include language enforcing appropriate non-disclosure agreements.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

#### **4.1.2.2 Position Categorization**

The USPTO shall assign a risk designation to all positions and establish screening criteria for individuals filling those positions. Position descriptions shall be written or annotated to reflect specific security responsibilities and position sensitivity levels. Within this context, the phrase “specific security responsibilities” refers to employee obligations to protect sensitive data and to use such data and information derived from it only in the execution of official duties. The USPTO shall review and revise position risk designations.

#### **4.1.2.3 Personnel Screening (Background Investigations)**

In accordance with *Executive Order 10450, Security Requirements for Government Employees*, 5 CFR 731, 732, 735 all employees shall be subject to an appropriate background check prior to permitting access to AIS and computer resources. Background investigations ensure that all employees and contractor employees are designated with position-sensitivity levels that are commensurate with the responsibilities and risks associated with the position. The Background Investigation may consist of a National Agency Check (NAC), subject interview, written inquiries, record searches, credit check, and personal interviews with selected sources covering employment, residence, education, and law enforcement agencies during the most recent five-year period, but not less than two years with a credit check up to seven years. Background investigations shall be completed and favorably adjudicated for personnel assigned to these positions prior to allowing access to sensitive systems and networks. Contracts shall include language requiring background checks equivalent to National Agency Check with Investigation (NACI).

For contractor employees, the risk designation or sensitivity level of the contract determines the type of background investigation that shall be conducted for the individual performing the work. Regardless of the risk or sensitivity rating of the contract, Personal Identity Verification under *Homeland Security Presidential Directive-12 (HSPD-12)* and in accordance with the *FIPS 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors* may dictate a more stringent background investigation for individuals performing work on the contract.

#### **4.1.2.4 Personnel Separation or Transfer**

Upon employee or contractor employee termination or other departure, all access and privileges to systems, networks, and facilities shall be revoked. An exit interview(s) shall be conducted and all organizational information system-related property (e.g., keys, identification/purchase/travel cards, building passes) shall be returned immediately. All information and official records stored on AIS that are created by the employee or contractor employee shall be made accessible to their supervisor.

When an employee or contractor employee is transferred or reassigned to other positions within the agency, the USPTO shall review AIS and facility access authorizations and initiate appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts, and changing system access authorizations). User system access and privileges shall also be reviewed based on the risk assumed with the new role.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

#### **4.1.2.5 Access Agreements**

For employees, appropriate divisions of responsibility and separate duties are established, as needed, to eliminate conflicts of interest in the responsibilities and duties of individuals. The concept of least privilege shall be employed for specific duties and AIS (including specific ports, protocols, and services) in accordance with RAs as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.

For contractor employees, the contract risk level shall be determined based on the following criteria such that each contractor employee is provided specific system access commensurate with the risk or sensitivity assigned the contract.

- Risk or sensitivity of the work being planned;
- Risk or sensitivity of the facility upon or in which the work is to be performed;
- Risk or sensitivity level of the IT system to which personnel have access;
- Level of access privileges to an IT system;
- When the contracted activities are to be performed (during or outside normal working hours); and,
- Extent that a government escort will be both necessary and available to the contract employees present in the facility or while IT access is required.

Effective administration of users' computer access is essential to maintaining system security. Administration of system users focuses on identification, authentication, and access authorizations. The USPTO shall require a process of auditing and otherwise periodically verifying the legitimacy of current accounts and access authorizations. In addition, the process must address the timely modification or removal of access and associated issues for employees who are reassigned, promoted, terminated, or who retire.

#### **4.1.2.6 Third-Party Personnel Security**

Compliance with the personnel security requirements for third-party providers established by the Office of Acquisition Management and monitoring provider compliance shall be implemented to ensure adequate security. Third party providers include service bureaus, contractors, and other organizations providing AIS development, information technology services, outsourced applications, and network and security management.

#### **4.1.2.7 Personnel Sanctions**

Disciplinary or adverse actions shall be administered against employees or contractors who fail to comply with established security policies and procedures. The *USPTO Discipline and Penalties Policy* maintained by the Office of Human Resources addresses disciplinary action.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

## **4.2 Awareness and Training**

### **4.2.1 Purpose/Requirements**

The *FISMA* requires each federal agency to provide mandatory periodic information security training to all employees involved in the use or management of federal computer systems. The *OMB Circular A-130* requires that training be completed prior to the granting of access and be provided for periodic refreshment. Refer to NIST SP 800-16 *Information Technology Security Training Requirements: A Role and Performance-Based Model* for more detail on this topic.

This Operational Control ensures that (i) managers and users of organizational AIS are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational AIS; and (ii) organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities. Education is explicitly not a component.

A continuum learning model can be used to define the IT security learning needed as a person assumes different roles within the USPTO and different responsibilities in relation to IT systems. The type of learning that individuals need becomes more comprehensive and detailed at the top of the continuum. Thus, beginning at the bottom, all employees need awareness. Training (represented by the two bracketed layers “Security Basics and Literacy” and “Roles and Responsibilities Relative to IT Systems”) is required for individuals whose role in the organization indicates a need for special knowledge of IT security threats, vulnerabilities, and safeguards. The “Education and Experience” layer applies primarily to individuals who have made IT security their profession.

This *IT Security Handbook* and referenced policy and process documents address each of the Security Awareness and Training controls as noted in Table 4-2:.

**Table 4-2: Awareness and Training Controls**

<b>Awareness and Training Controls</b>				
<b>Control Number</b>	<b>Control Name</b>	<b>Control Baselines</b>		
		<b>Low</b>	<b>Moderate</b>	<b>High</b>
AT-1	Security Awareness and Training Policy and Procedures	AT-1	AT-1	AT-1
AT-2	Security Awareness	AT-2	AT-2	AT-2
AT-3	Security Training	AT-3	AT-3	AT-3
AT-4	Security Training Records	AT-4	AT-4	AT-4

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

## **4.2.2 Policy**

### **4.2.2.1 Security Awareness and Training**

In accordance with *NIST SP 800-53, Rev.1*, the USPTO shall develop, disseminate, and periodically review/update: (i) a formal documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

### **4.2.2.2 Security Training and Awareness**

It is important that all USPTO AIS users are provided security education and awareness training as part of their initiation and on a reoccurring basis. As a result, the following guidelines have been developed:

- New USPTO users shall receive an initial security awareness course before being granted permanent access to USPTO systems and networks
- An awareness class shall be attended within 30 days of receiving logical system access
- All USPTO users shall receive annual (refresher) training in IT security awareness
- When there is a significant change in the AIS security environment or procedures additional training shall be provided
- Provide specialized security education and awareness training for all security positions and roles that is commensurate with the individual's duties and responsibilities. The Commerce Learning Center has specific role-based training available for use
- The IT Security Awareness, Training, and Education component shall be consistent with the methodology of *NIST SP 800-50, Building an Information Technology Security Awareness and Training Program*, and apply to all USPTO employees, contractor employees, remote researchers and collaborators working on USPTO projects, and temporary guests of USPTO. The components shall include awareness activities, basics and literacy training activities for general users, and role-based training for specialized users. At a minimum, the user shall understand the following IT security topics (this is not an inclusive list):
  - IT security threats to USPTO users and systems
  - USPTO IT security policies
  - Information and data sensitivity
  - USPTO adverse actions for policy and procedure violations

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- Social engineering threats
- Password management
- Physical security for IT systems
- Anti-virus software
- Incident handling and reporting
- Risk management
- Copyright compliance
- Contingency planning (system and data backup and recovery)
- Media disposal
- Labeling information and media

#### **4.2.2.3 Security Training Records**

The *OMB Memoranda M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*, requires the USPTO to report the following information:

- The number of agency employees during the fiscal year.
- The number and percentage of agency employees who have received IT security training during the fiscal year.
- The number of agency employees with significant IT security responsibilities.
- The number and percentage of agency employees with significant IT security responsibilities that received specialized training.
- Descriptions of the USPTO IT security training provided.
- Total costs for training (to include labor and materials for training operations and student related training time and travel).

As a result, the USPTO shall document and monitor individual AIS security training activities including basic security awareness training and specific AIS security training.

Each employee shall have a record which contains all security awareness training activities used with each program component. The following employee and contractor employee information shall be tracked:

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- Unique identifier (e.g., e-mail address)
- Role and organization to assess significant security responsibilities
- Training completed with course description
- Date each training course was completed to distinguish training completed year to year
- Cost of training for labor, materials, facilities, infrastructure and travel

Refer to the *IT Security Training and Awareness Policy* for more details.

## **4.3 Physical and Environmental Protection**

### **4.3.1 Purpose/Requirements**

This operational control ensures that USPTO systems are adequately protected through (i) limiting physical access to AIS, equipment, and the respective operating environments to authorized individuals; (ii) protecting the physical plant and support infrastructure for AIS; (iii) providing supporting utilities for AIS; (iv) protecting AIS against environmental hazards; and, (v) providing appropriate environmental controls in facilities containing AIS.

Security requirements for computer facilities must include physical construction, fire protection, access controls, and environmental controls. Facility security measures are developed and implemented based on the level of risk to the computer and information resources as identified by an assessment of risk. Facilities and rooms under OCIO control containing system hardware and software, such as local area network rooms or telephone closets, are secured, where possible, to ensure that they are accessible to authorized personnel only.

Facilities which contain AIS require physical security measures to ensure proper and timely operation, help protect the facilities, safeguard the integrity of information, and ensure the safety of personnel. Facilities which contain AIS and media storage areas shall be protected from theft, alteration, damage by fire, dust, water, and other contaminants, power loss, and unauthorized disruption of operation. The extent of physical security measures needed is determined by the results of a risk analysis and/or a physical security survey.

This *IT Security Handbook* and referenced policy and process documents address each of the Physical and Environmental Protection controls as noted in Table 4-3.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

**Table 4-3 Physical and Environmental Controls**

<b>Physical and Environmental Controls</b>				
<b>Control Number</b>	<b>Control Name</b>	<b>Control Baselines</b>		
		<b>Low</b>	<b>Moderate</b>	<b>High</b>
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	PE-2	PE-2	PE-2
PE-3	Physical Access Control	PE-3	PE-3	PE-3 (1)
PE-5	Access Control for Display Medium	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	PE-6	PE-6 (1)	PE-6 (1) (2)
PE-7	Visitor Control	PE-7	PE-7 (1)	PE-7 (1)
PE-8	Access Records	PE-8	PE-8	PE-8 (1) (2)
PE-9	Power Equipment and Power Cabling	Not Selected	PE-9	PE-9
PE-10	Emergency Shutoff	Not Selected	PE-10	PE-10 (1)
PE-11	Emergency Power	Not Selected	PE-11	PE-11 (1)
PE-12	Emergency Lighting	PE-12	PE-12	PE-12
PE-13	Fire Protection	PE-13	PE-13 (1) (2) (3)	PE-13 (1) (2) (3)
PE-14	Temperature and Humidity Controls	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	Not Selected	PE-18	PE-18 (1)

## **4.3.2 Policy**

### **4.3.2.1 Physical and Environmental Protection**

In accordance with *NIST SP 800-53, Rev.1*, the USPTO shall develop, disseminate, and periodically review/update: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

Physical security is concerned with the measures to prevent unauthorized physical access to equipment, facilities, material, information, and documents. Physical security also safeguards assets against espionage, sabotage, damage, tampering, theft, and other covert acts.

Hardware, software, telecommunications, documentation, and all sensitive information handled by a system shall be adequately protected to prevent unauthorized access, use, modification, disclosure, or destruction.

Before conducting sensitive operations at any location, security planning must consider physical security and AIS security as part of the accreditation process. The two types of physical security are facility and environmental security.

Facility security is concerned with preventing unauthorized access to systems protected within a given physical perimeter.

Environmental security is concerned with measures to prevent USPTO systems from being damaged due to environmental factors such as water and fire.

Refer to the *USPTO AAO 207-1*<sup>5</sup> for a complete description of all physical and environmental protection policies and procedures.

#### **4.3.2.2 Physical Access**

All physical access points (including designated entry/exit points) to facilities containing AIS shall be controlled (except for those areas within the facilities officially designated as publicly accessible), and individual access authorizations are to be verified before granting access to the facilities. Access shall be controlled to areas officially designated as publicly accessible, as appropriate, in accordance with the assessment of risk. Physical access procedures include:



- Only authorized employees and contractor employees shall be granted entrance in a USPTO or contractor data center. Visitors shall sign in and be escorted...24/7.
- Physical access to all business and mission critical systems and information shall be monitored to detect and respond to incidents. Real-time physical intrusion alarms and surveillance equipment are monitored and automated mechanisms employed to recognize potential intrusions and initiate appropriate response actions.
- Physical access to all USPTO or contractor data centers shall be documented and managed.

---

<sup>5</sup> Currently the *USPTO AAO 207-1* document is under development. Once it is developed and implemented, a notification will be sent to all relevant divisions.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- The process for granting card and/or key access to AIS facilities shall include the approval of the person responsible for the facility.
- All physical access points (including designated entry/exit points) to those facilities containing business and mission critical systems shall be controlled, and individual access authorizations shall be verified before granting access to the facilities.
- Access to areas officially designated as publicly accessible shall be controlled in accordance with the organization's assessment of risk.
- Physical access devices (e.g., keys, locks, combinations, card readers) shall be used to control entry to facilities containing business and mission critical systems.

#### **4.3.2.3 Access Control for Display Medium**

Physical access to AIS devices that display information within agency facilities shall be controlled.



#### **4.3.2.4 Visitor Control**

Physical access to AIS shall be controlled by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible. Visitor access records shall be maintained for all AIS facilities. The record shall include (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Visitors (including government contractors) shall be authenticated prior to authorizing access to facilities or areas other than areas designated as publicly accessible and shall be escorted in card access controlled areas of AIS facilities at all times. A controlled area is defined as a room, office, building, or other form of facility to which access is monitored, controlled, or restricted. Admittance to a controlled area is limited to persons who have official business within the area.

#### **4.3.2.5 Equipment Security**

Equipment<sup>6</sup> shall be protected by implementing the following procedures:

- The USPTO shall protect power equipment and power cabling for each AIS from damage and destruction.



---

<sup>6</sup> USPTO references to equipment security are specific to devices maintained and stored within data center facilities.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- For moderate- and mission critical AIS, cabling paths shall be redundant and parallel with existing power cabling paths.
- Short-term uninterruptible power supplies (UPSs) shall be provided to enable a systematic shutdown of AIS components due to a power source loss. For high sensitivity systems, a long-term alternate power supply shall be provided that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.
- In addition to protecting the power supply, there shall be specific locations within an AIS facility for shutting off power to any AIS component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment. The master power switch or emergency cut-off switch shall be prominently marked and protected by a cover to prevent accidental shutoff.

#### **4.3.2.6 Fire Prevention**

Fire suppression and detection devices/systems shall be employed and maintained that can be activated within AIS facilities in the event of a fire. Within all AIS facilities (continuously or non-continuously staffed), fire suppression and detection devices/systems activate automatically in the event of a fire, and fire suppression and detection devices/systems provide automatic notification of any activation to the organization and emergency responders.



#### **4.3.2.7 Water Damage Protection**

Within AIS facilities, the master water shutoff valves shall be accessible, working properly, and properly marked and location(s) known to key personnel to ensure that the business and mission critical systems are protected from water damage resulting from broken plumbing lines or other sources of water leakage.

#### **4.3.2.8 Supporting Utilities**

In addition to providing equipment security and fire protection, the following procedures shall be performed to ensure AIS availability:

- Within all AIS facilities, mechanisms measuring and regulating acceptable levels of humidity and temperature shall be monitored containing business and mission critical systems. Automatic reporting of anomalies shall be in place and operational.
- Automatic emergency lighting systems shall be employed and maintained that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- AIS-related items (i.e., hardware, firmware, software) entering and exiting the facility shall be controlled and appropriate records of those items maintained.
- Appropriate AIS security controls at alternate work sites shall be employed.
- All AIS components are positioned to minimize damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

## **4.4 Incident Response**

### **4.4.1 Purpose/Requirements**

The *FISMA* requires all agencies to report security incidents to a federal incident response center. The response center, known as US-CERT, is located within the Department of Homeland Security (DHS). As a result, it is critical that the USPTO have an established Incident Response policy and procedures.

This operational control (i) establishes an operational incident handling capability for organizational AIS that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) tracks, documents, and reports incidents to appropriate organizational officials and/or authorities.

A security incident is any event or condition that has the potential to impact the security or accreditation of systems. These incidents may result from intentional or unintentional actions and may include loss or theft of computer media, introduction of malicious code, unauthorized attempts to gain access to USPTO information or the failure of system security functions to perform as expected. Detailed incident reporting and response procedures are contained in the *OCIO's Computer Incident Response Procedures* document. Examples of potential compromises to information resource symptoms that all system users should be aware of include, but are not limited to:

- Password changes the user did not initiate (user cannot log in) or requests to share the user's password,
- E-mail activity to the user or that is received in the user's mailbox from an unknown source.
- Responses to e-mail that were not sent by the user.
- Large volumes of spam, or large numbers of messages the user did not send.
- Browser home page changes or pop-up ads that cannot be closed.
- New desktop icons appearing at login.
- Inability to connect to USPTO or Internet servers (web- or application-sites).

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- Sudden workstation slowdowns.
- File additions, changes, or deletions.
- Noticeable decreases in hard drive space.

The *USPTO IT Security Handbook* and referenced policy and process documents address each of the Incident Response controls as noted in Table 4-4.

**Table 4-4 Incident Response Controls**

Incident Response Controls				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
IR-1	Incident Response Policy and Procedures	IR-1	IR-1	IR-1
IR-2	Incident Response Training	Not Selected	IR-2	IR-2 (1)
IR-3	Incident Response Testing and Exercises	Not Selected	IR-3	IR-3 (1)
IR-4	Incident Handling	IR-4	IR-4 (1)	IR-4 (1)
IR-5	Incident Monitoring	Not Selected	IR-5	IR-5 (1)
IR-6	Incident Reporting	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	IR-7	IR-7 (1)	IR-7 (1)

## 4.4.2 Policy

### 4.4.2.1 Incident Response

In accordance with *NIST SP 800-53, Rev.1*, the USPTO shall develop, disseminate, and periodically review/update: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

An incident is the act of violating an explicit or implied security policy. These include but are not limited to:

- attempts (either failed or successful) to gain unauthorized access to a system or its data
- unwanted disruption or denial of service
- the unauthorized use of a system for the processing or storage of data
- changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

### 4.4.2.2 Incident Response Training

Agency personnel shall receive training specific to their AIS incident response roles and responsibilities. For high sensitivity systems, the USPTO shall incorporate simulated events.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

#### **4.4.2.3 Incident Response Testing and Exercises**

The incident response capability for AIS shall be tested at least annually using tests and exercises defined by the USPTO in its procedures to determine the incident response effectiveness and document the results. For high sensitivity AIS, automated mechanisms are employed as much as possible to more thoroughly and effectively test the incident response capability.

#### **4.4.2.4 Incident Handling and Monitoring**

The USPTO CIRT shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, recovery, and monitoring. The incident handling processes are described as follows:

- **Preparation** – USPTO will be prepared to respond before an incident occurs to be as ready as possible to respond to incidents and limit the potential for damage by ensuring that response plans are familiar to all staff.
- **Detection and Analysis** – USPTO will use an incident identification process that involves 1) validating the incident, 2) if an incident has occurred, identify its nature, 3) identifying and protecting the evidence, and 4) logging and reporting the event or incident.
- **Containment** – The immediate objective for USPTO will be to limit the scope and magnitude of an incident as quickly as possible, rather than to allow the incident to continue in order to gain evidence for identifying and/or prosecuting the perpetrator. It may occur that a system will need to be 1) shut down entirely, 2) disconnected from the network, or 3) allowed to continue to run in its normal operational status by exception (so that any activity on the system can be monitored). For all categories of incidents, the decision to take any of these actions will be made by the USPTO CIRT, in consultation with the Executive Management Council or designated Business Unit representatives. In either case the decision to take action will be based on the risk to assets threatened by the incident and the impact of continued loss of Business production based on the IT system affected. For high sensitivity AIS, automated mechanisms shall be employed to support incident handling.
- **Eradication** – After containing the damage from a computer security incident, USPTO will remove the cause of the incident. Removal of incident artifacts (e.g., Trojan horses, viruses) from all systems and media (primary and back-up) using proven commercial eradication applications or other means will take into consideration the seriousness of the risk and the cost.
- **Recovery** – USPTO will restore affected systems to their normal operational mission status as soon as possible, in accordance with established IT CPs.
- **Monitoring** – USPTO will follow up on an incident after recovery to identify systemic weaknesses, to prevent future incidents from occurring, and to improve incident handling procedures. For high sensitivity AIS, the USPTO employs automated mechanisms to

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

assist in the tracking of security incidents and in the collection and analysis of incident information.

To protect against potential computer incidents:

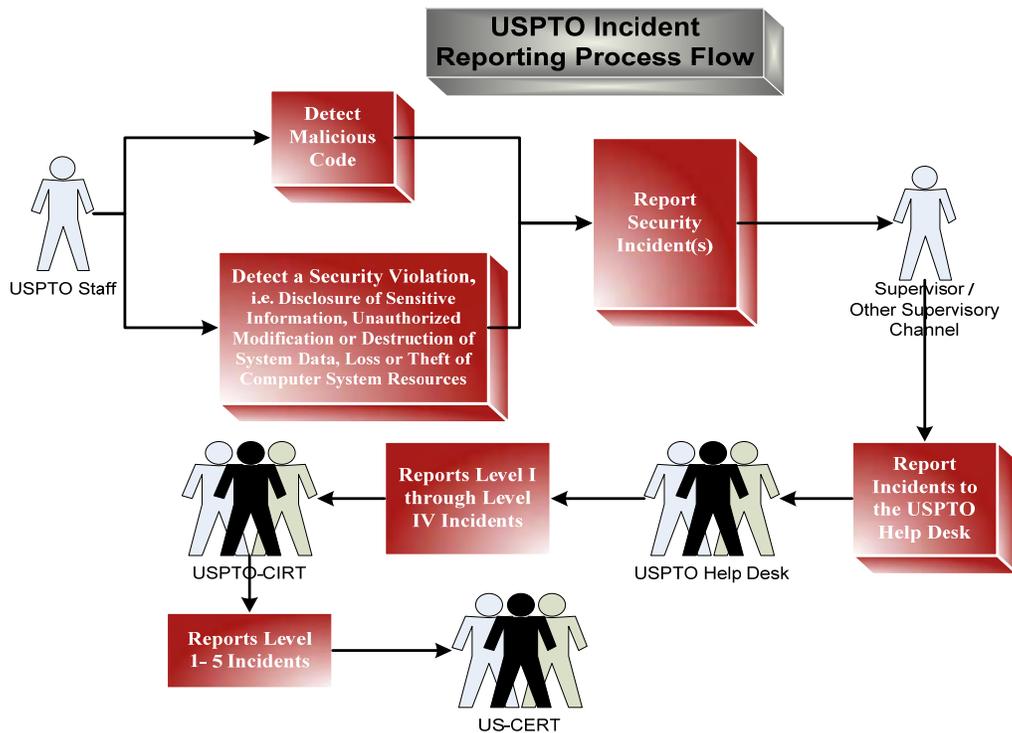
- All USPTO Internet connections shall have network-based intrusion detection systems (IDS) in place and functioning, with the latest patches installed.
- All Internet-accessible USPTO Web servers shall have host-based intrusion detection systems in place and functioning with the latest patches installed.
- Both host-based and network-based intrusion detection systems shall be deployed to provide near-real-time detection to alert USPTO of suspicious activity in order to better detect malicious code executed against USPTO systems.
- All production servers, network devices, and major applications (i.e., database, e-mail) shall have normal auditing processes enabled to detect possible computer incidents.  
**NOTE:** Desktop workstations are not required to have auditing enabled.
- Other detection means that shall be enabled include alarm and alert functions such as logging of firewalls and other network perimeter security devices.

#### **4.4.2.5 Incident Reporting and Response**

All employees and contractor employees shall be responsible for reporting physical, IT security violations, and/or possible virus infections that they are aware of to their supervisor(s) or other appropriate supervisory channels and promptly call or e-mail the USPTO Helpdesk. For incident reporting during non-standard hours, please contact the Helpdesk at 571-272-9000 (5:30 AM - 12:00 AM). Security Incidents are forwarded from the USPTO Help Desk to the USPTO CIRT. The USPTO CIRT shall use a set of formal mechanisms and procedures that make it possible for quick, consistent, and decisive action when an incident occurs.

Figure 4-1 illustrates the incident reporting process for USPTO employees and contractor employees, should they encounter a security incident or violation.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**



**Figure 4-1: USPTO Incident Report Process**

When a USPTO employee or contractor employee reports an incident, the following information shall be provided:

1. Agency name
2. Point of contact information including name, telephone, and email address
3. Incident Category Type (e.g., CAT 1, CAT 2, etc., see table below)
4. Incident date and time, including time zone
5. Source IP, port, and protocol
6. Destination IP, port, and protocol
7. Operating System, including version, patches, etc.
8. System Function (e.g., DNS/web server, workstation, etc.)

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

9. Antivirus software installed, including version, and latest updates
10. Location of the system(s) involved in the incident (e.g., Washington DC, Los Angeles, CA)
11. Method used to identify the incident (e.g., IDS, audit log analysis, system administrator)
12. Impact to agency
13. Resolution

It is important to note that reporting should not be delayed in order to gain additional information.

In order to effectively report and respond to computer security incidents, the USPTO CIRT has categorized incidents into seven (7) incident categories to determine the appropriate response and course of action. Incidents fall into a category where the USPTO will treat each incident as a possible attempt at gaining unauthorized access to resources or information. USPTO shall comply with US-CERT guidelines regarding incident response reporting and NIST SP 800-61, *Computer Incident Handling Guide*.

The incident severity levels and reporting timeframes shall be:

Category	Name	Description	Reporting Timeframe
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Not Applicable; this category is for each agency's internal use during exercises.
CAT 1	*Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource	Within one (1) hour of discovery/detection.
CAT 2	*Denial of Service (DoS)	An attack that <i>successfully</i> prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	*Malicious Code	<i>Successful</i> installation of malicious software (e.g., virus, worm, Trojan horse, or other	Daily Note: Within one (1) hour of discovery/detection if

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

Category	Name	Description	Reporting Timeframe
		code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been <i>successfully quarantined</i> by antivirus (AV) software.	widespread across agency.
CAT 4	*Improper Usage	A person violates acceptable computing use policies.	Weekly
CAT 5	Scans/Probes/Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly Note: If system is classified, report within one (1) hour of discovery.
CAT 6	Investigation	<i>Unconfirmed</i> incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

**NOTE:** IT security incident report information shall be treated as sensitive information and safeguarded as such. Access to IT security incident information shall be restricted and stored in a secured area. The USPTO CIRT shall prepare a final report following the completion of all incident response activities and the affected system(s) declared operational.

## 4.5 Media Protection

### 4.5.1 Purpose/Requirements

This operational control (i) protects AIS media, both paper and digital; (ii) limits access to information on AIS media to authorized users; and (iii) sanitizes or destroys AIS media before disposal or release for reuse.

The *USPTO IT Security Handbook* and referenced policy and process documents address each of the Media Protection controls as noted in Table 4-5.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

**Table 4-5 Media Protection Controls**

<b>Media Protection Controls</b>				
<b>Control Number</b>	<b>Control Name</b>	<b>Control Baselines</b>		
		<b>Low</b>	<b>Moderate</b>	<b>High</b>
MP-1	Media Protection Policy and Procedures	MP-1	MP-1	MP-1
MP-2	Media Access	MP-2	MP-2 (1)	MP-2 (1)
MP-4	Media Storage	Not Selected	MP-4	MP-4
MP-5	Media Transport	Not Selected	MP-5 (1) (2) (4)	MP-5 (1) (2) (3)
MP-6	Media Sanitization and Disposal	MP-6	MP-6	MP-6 (1) (2)

## **4.5.2 Policy**

### **4.5.2.1 Media Protection**

In accordance with *NIST SP 800-53, Rev.1*, the USPTO shall develop, disseminate, and periodically review/update: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.



### **4.5.2.2 Sensitive Information Handling**

USPTO employees and contractor employees shall be responsible for (i) the proper control, classification, handling and marking of sensitive information residing on their computers and on removable media that they possess; and (ii) the control, storage and destruction of printouts of sensitive information that they produce as well as non-record electronic copies of such information.

For high sensitivity data, all electronic and non-electronics records shall be labeled as **Sensitive But Unclassified**. Contact the ITSMG for additional guidance identifying high-sensitivity data. Examples of high-sensitivity data include:

- AIS Security documentation such as *Security Plans, Contingency Plans, Emergency Operations Plans, Incident Reports, Risk and Security Control Assessment Reports*
- Information related to law enforcement investigations

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- Agency mission critical information which includes trademark and patent applications

**NOTE:** Patent applications received with National Security markings shall be processed manually and their sensitive content will not be entered into any USPTO electronic systems of lower classification. Patent applications deemed to be of National Security interest by external reviewing agencies shall be processed manually and their sensitive content will be removed from any USPTO electronic systems, unless they are classified for that level of processing.

Anything ordered to be filed under seal pursuant to a protective order issued or made by any court or by the Trademark Trial and Appeal Board in any proceeding involving a trademark application or registration shall be kept confidential and shall not be made available for public inspection or copying, unless otherwise ordered by the court or the Board or the party protected by the order voluntarily discloses any of the subject matter.

Questions concerning identification and access to sensitive information should be directed to the appropriate program policy office after consulting written policy guidance, e.g., *MPEP*, *TMEP*, etc. Refer to the *IT Privacy Policy* for additional policy and process guidance.

#### **4.5.2.3 Media Access and Control**

Access to USPTO AIS media shall be restricted to only authorized individuals based on the sensitivity of the data. Furthermore, appropriate physical security and access control measures shall be established for facilities storing AIS media, including off-site facilities. For moderate- and high-sensitivity AIS, automated mechanisms shall be employed that restrict access to media storage areas and to audit access attempts and access granted.

#### **4.5.2.4 Media Storage and Transport**

All moderate- and high-sensitivity AIS media shall be securely stored within controlled areas and adequately protected during transport outside of controlled areas, including limiting transport to only authorized personnel. All computer systems media containing information considered to be federal records shall be saved in accordance with applicable records management laws and regulations. Refer to the *IT Privacy Policy*, *Electronic Records Management Standard* (as re-titled in May 2007), and the *USPTO Comprehensive Records Schedule* for additional policy and process guidance.

#### **4.5.2.5 Sanitization and Disposal of Information**

All USPTO AIS media shall be sanitized in accordance with approved disposal methods. For high sensitivity AIS, media sanitization shall be tracked, documented, verified, and the equipment and procedures periodically tested. Refer to the *Electronics Records Management Standard* for specific policy and process guidance.

This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.

## 4.6 System and Information Integrity

### 4.6.1 Purpose/Requirements

This operational control (i) identifies, reports, and corrects information and AIS flaws in a timely manner; (ii) provides protection from malicious code at appropriate locations within organizational AIS; and (iii) monitors AIS security alerts and advisories and takes appropriate actions in response.

The *USPTO IT Security Handbook* and referenced policy and process documents address each of the System and Information Integrity controls as noted in Table 4-6.

**Table 4-6 System and Information Integrity Controls**

System and Information Integrity Controls				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
SI-1	System and Information Integrity Policy and Procedures	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	Malicious Code Protection	SI-3	SI-3 (1) (2)	SI-3 (1) (2)
SI-4	Information System Monitoring Tools and Techniques	Not Selected	SI-4 (4)	SI-4 (2) (4) (5)
SI-5	Security Alerts and Advisories	SI-5	SI-5	SI-5 (1)
SI-8	Spam Protection	Not Selected	SI-8	SI-8 (1)
SI-9	Information Input Restrictions	Not Selected	SI-9	SI-9
SI-10	Information Accuracy, Completeness, Validity, and Authenticity	Not Selected	SI-10	SI-10
SI-11	Error Handling	Not Selected	SI-11	SI-11
SI-12	Information Output Handling and Retention	Not Selected	SI-12	SI-12

### 4.6.2 Policy

#### 4.6.2.1 System and Information Integrity

In accordance with *NIST SP 800-53, Rev1*, the USPTO shall develop, disseminate, and periodically review/update: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

#### **4.6.2.2 Flaw Remediation**

In order to address software and hardware flaws that affect AIS, the following corrective actions shall be performed: add in spy ware

- Identify AIS containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws).
- Promptly test newly released relevant security patches, service packs, and hot fixes for effectiveness and potential side effects on AIS before installation.
- Remediate or eliminate risks which occur as a result of flaws discovered during security assessments, continuous monitoring, incident response activities, or AIS error handling.

An agency process is in place to identify, track, and report security patch management that is consistent with the methodology described in *NIST SP 800-40, Procedures for Handling Security Patches*. The process addresses the following requirements for a patch management program:

- Establish a mechanism for ensuring accountability for patch management. Resources committed to this activity should be appropriate to the size and scope of the mission.
- Each business area should centralize patch management leadership to assure that suitable attention is given in a timely way to patches for all systems, and to minimize duplication of patch management functions across the operating unit.
- Document business area procedures to identify, track, test (as appropriate), and disseminate security-related information concerning patches.
- Ensure compliance with these procedures to guide patch management throughout the business area.

#### **4.6.2.3 Malicious Code Protection**

All AIS shall be protected from malicious code by using approved countermeasures designed to minimize or eliminate the risk of introducing malicious code commensurate with the sensitivity of the information that resides on the system.

All application developers shall adhere to the Secure Application Development Policy<sup>7</sup>. This policy establishes minimum practices to ensure secure code is developed and implemented on all USPTO IT systems during project development in the USPTO SDLC.

All e-mail servers and workstations shall implement real-time anti-virus software protection for both inbound and outbound e-mails and attachments. Other types of non-e-mail servers shall scan all files and data when they are first introduced onto the system and at least once every

---

<sup>7</sup> Currently in draft format.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

week thereafter to detect viruses that may have been previously undetectable due to the timeliness and availability of anti-virus signatures.

For moderate- and high-sensitivity AIS, the USPTO shall manage and automatically update protective software. Refer to the *Anti-Virus Policy* for additional policy and process guidance.

#### **4.6.2.4 Information System Monitoring Tools and Techniques**

For moderate- and high-sensitivity AIS, tools and techniques shall be employed to monitor events, detect attacks, and provide identification of unauthorized use of the system. To protect the network and AIS from intrusion and unauthorized access, the USPTO shall:

- Maintain both network-based and host-based IDSs.
- Determine the intrusion detection architecture based on assessment of risk and use of cost-effective intrusion detection measures.
- Monitor IDSs on a 24x7 basis.
- Base staffing for intrusion detection monitoring on assessment of risk and use of cost-effective staffing measures.

#### **4.6.2.5 Security Alerts and Advisories**

AIS security alerts and advisories from the US-CERT shall be monitored on a regular basis, issued to appropriate personnel, and appropriate actions taken in response to alerts and advisories. The types of actions to be taken in response to security alerts and advisories shall be documented. For high sensitivity systems, automated mechanisms shall be employed to make security alert and advisory information available throughout the agency as needed.

#### **4.6.2.6 Spam Protection**

Spam and Spy ware protection shall be deployed on moderate- and high-sensitivity AIS. Spam protection mechanisms shall be employed at critical AIS entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. Spam protection mechanisms shall be continuously updated and used to detect and take appropriate action on unsolicited messages transported by electronic mail, electronic mail attachments, Internet accesses, or other common means. Refer to the *Anti-Virus Policy* for additional policy and process guidance.

#### **4.6.2.7 Information Input/Output and Error Handling**

The USPTO shall ensure the integrity of data that resides on AIS through the establishment of input restrictions, information verification, error handling, and output handling and retention. As such, all AIS shall:

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- Be configured to restrict the information input for moderate- and high-sensitivity AIS to authorized personnel.
- Check data for accuracy, completeness, validity, and authenticity with data integrity and validation controls and establish rules for checking the valid syntax of AIS inputs (e.g., character set, length, numerical range, acceptable values) that are in place to verify that inputs match specified definitions for format and content.
- Identify and handle error conditions in an expeditious manner without providing information that could be exploited by adversaries.

Refer to the USPTO *Comprehensive Records Schedule* and Media Protection control policies for additional process guidance.

## 4.7 Maintenance

### 4.7.1 Purpose/Requirements

This operational control ensures that USPTO performs periodic and timely maintenance on organizational AIS and provides effective controls on the tools, techniques, mechanisms, and personnel used to conduct AIS maintenance.

This *IT Security Handbook* and referenced policy and process documents address each of the Maintenance controls as noted in Table 4-7:.

**Table 4-7: Maintenance Controls**

Maintenance Controls				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
MA-1	System Maintenance Policy and Procedures	MA-1	MA-1	MA-1
MA-2	Controlled Maintenance	MA-2	MA-2 (1)	MA-2 (1) (2)
MA-3	Maintenance Tools	Not Selected	MA-3	MA-3 (1) (2) (3)
MA-4	Remote Maintenance	MA-4	MA-4 (1) (2)	MA-4 (1) (2) (3)
MA-5	Maintenance Personnel	MA-5	MA-5	MA-5
MA-6	Timely Maintenance	Not Selected	MA-6	MA-6

### 4.7.2 Policy

#### 4.7.2.1 System Maintenance

In accordance with *NIST 800-53, Rev1*, USPTO shall develop, disseminate, and periodically review/update: (i) a formal, documented, AIS maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

compliance; and (ii) formal, documented procedures to facilitate the implementation of the AIS maintenance policy and associated system maintenance controls.

#### **4.7.2.2 Controlled Maintenance**

Each SO shall be responsible for scheduling, performing, documenting, and reviewing records of preventative and regular maintenance on AIS in accordance with agency requirements. Only authorized personnel shall be allowed to perform maintenance on any AIS. Furthermore, each moderate- and high-sensitivity AIS shall have a maintenance record for each system that includes the following information:

1. Date and time of maintenance
2. Name of individual(s) performing the maintenance
3. Description of maintenance performed
4. List of equipment removed or replaced

#### **4.7.2.3 Maintenance Tools**

Maintenance tools to be used for any activity on an AIS shall be approved, controlled, and monitored. All media containing diagnostic and test programs shall be verified for malicious code before the media is used. In addition, all maintenance tools shall be restricted to authorized personnel only. For all moderate- and high-sensitivity AIS, maintenance support and spare parts shall be accessible within a timely manner following a system failure.

#### **4.7.2.4 Remote Maintenance**

All maintenance and diagnostic activities executed remotely in support of an AIS shall be approved, controlled, and monitored. For moderate- and high-sensitivity AIS, all remote maintenance and diagnostic sessions shall be audited and appropriate personnel shall review the maintenance records of the remote sessions and manage the installation and use of remote maintenance and diagnostic links for the AIS. The installation and use of remote maintenance and diagnostic links shall be documented in the AIS SSP.

### **4.8 Contingency Planning**

#### **4.8.1 Purpose/Requirements**

This operational control ensures that USPTO establishes, maintains, and effectively implements plans for emergency response, backup operations, and post-disaster recovery for organizational AIS to ensure the availability of critical information resources and continuity of operations in emergency situations.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

Having well-planned and tested procedures for contingency operations and disaster recovery will make the difference between continued business processes and struggling to replace lost data or systems along with the associated inability to continue to work. Contingency Planning develops procedures that provide continued essential business processes if systems or information technology support are interrupted.

Each AIS shall have a viable and logical Contingency Plan (CP). This Plan shall be routinely reviewed, tested, and updated to:

- Minimize damage and disruption caused by undesirable events
- Provide for continued performance of essential system and computer processing operations, services, and mission-critical functions

The CP shall provide reasonable assurance that critical data processing support can be continued or quickly resumed, if normal operations are interrupted. The SSP shall reference the CP.

CPs shall include the following:

- Backup operations plans, procedures and responsibilities—to ensure that essential (mission-critical) USPTO operations will continue if normal activities are stopped for a period of time.
- Emergency response procedures—to civil disorder; fire; flood; natural disaster; bomb threat; or other incidents or activities where lives, property, or the capability to perform essential functions are threatened or seriously impacted.
- The lowest acceptable level of essential system or function operation—identified and ranked so that plan priorities may be made. This must include provisions for storage, maintenance, and retrieval of essential backup and operational support data.
- Post-incident recovery procedures and responsibilities—to facilitate the rapid restoration of normal operations at a primary site or, if necessary, at an alternate facility, following destruction, major damage, or other significant interruptions of the primary site.

The *Contingency Planning ITSS* provides guidance with preparing system CPs and templates in accordance with *NIST SP 800-34, Contingency Planning Guide for Information Technology Systems*.

This *IT Security Handbook* and referenced policy and process documents address each of the Contingency Planning controls as noted in Table 4-8.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

**Table 4-8 Contingency Planning Controls**

<b>Contingency Planning Controls</b>				
<b>Control Number</b>	<b>Control Name</b>	<b>Control Baselines</b>		
		<b>Low</b>	<b>Moderate</b>	<b>High</b>
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	CP-1
CP-2	Contingency Plan	CP-2	CP-2 (1)	CP-2 (1) (2)
CP-3	Contingency Training	Not Selected	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing and Exercises	Not Selected	CP-4 (1)	CP-4 (1) (2)
CP-5	Contingency Plan Update	CP-5	CP-5	CP-5
CP-6	Alternate Storage Site	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	Not Selected	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	Telecommunications Services	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	CP-9	CP-9 (1) (4)	CP-9 (1) (2) (3) (4)
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10	CP-10 (1)

## **4.8.2 Policy**

### **4.8.2.1 Contingency Planning**

In accordance with *NIST SP 800-53, Rev1*, USPTO shall develop, disseminate, and periodically review/update: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls. The *Contingency Planning ITSS*<sup>8</sup> addresses each security control within the Contingency Planning security control family.

---

<sup>8</sup> Currently, the *Contingency Plan ITSS* is in draft format.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

#### **4.8.2.2 Contingency Plan**

The USPTO shall develop and implement a CP for each AIS addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the agency shall review and approve the CP and distribute copies of the plan to key contingency personnel. Each CP shall be reviewed annually and revised to address any system or Agency changes encountered during plan implementation, execution, or testing. For moderate- and high-sensitivity AIS, CP development shall be coordinated with divisions responsible for related plans.

#### **4.8.2.3 Contingency Training**

All AIS personnel shall be trained in their contingency roles and responsibilities for each AIS and provided refresher training annually.

#### **4.8.2.4 Contingency Plan Testing and Exercises**

Tests and exercises shall be conducted for all AIS CPs at least annually to determine the plan's effectiveness and agency readiness. The tests and exercises shall include various USPTO elements responsible for related plans, i.e., Business Continuity/Disaster Recovery (BC/DR) and Incident Response. The test and exercise results shall be reviewed and appropriate corrective action taken by the respective roles as noted in the CP. All CPs shall be tested before any system is accredited. For moderate- and high-sensitivity AIS, CP testing is coordinated with divisions responsible for related plans.

#### **4.8.2.5 Alternate Storage and Processing Sites**

CPs shall identify alternate storage and processing sites and agreements shall be in place to permit storage and resumption of processing for AIS. For moderate- and high-sensitivity AIS, the site(s) shall be geographically separated from the primary storage site, accessibility problems to the alternate site(s) identified and mitigated, and priority-of-service provisions in place in accordance with availability requirements.

#### **4.8.2.6 Telecommunications Services**

All AIS shall have primary and alternate telecommunications services identified to support the system and have agreements in place to permit the resumption of system operations for critical mission/business functions when the primary telecommunications are not available. For moderate- and high-sensitivity AIS, each primary and alternate telecommunications service agreement contains priority-of-service provisions in accordance with the availability requirements and specifies that alternate telecommunications services do not share a single point of failure with primary telecommunications services.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

#### **4.8.2.7 Information System Backup**

The USPTO shall back-up AIS so they can be restored if they are lost or damaged. The frequency of backups shall be documented in the Operational Support Plan (OSP). At a minimum, AIS shall have incremental back-ups daily and full backups weekly. Furthermore, all moderate- and high-sensitivity AIS shall test backup information to verify media reliability and information integrity and protect backup information from unauthorized modification.

**NOTE:** Information stored on personal PCs - local hard drives -- is not backed up by a central organization. Employees are strongly encouraged to take steps to periodically back up all data or business-related information to their network drive(s), which are automatically backed up regularly.

#### **4.8.2.8 Information System Recovery and Reconstitution**

All AIS shall employ mechanisms with supporting procedures to allow the system to be recovered and reconstituted to a known secure state after a disruption or failure.

### **4.9 Configuration Management**

#### **4.9.1 Purpose/Requirements**

This operational control ensures that USPTO (i) establishes and maintains baseline configurations and inventories of organizational AIS (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establishes and enforces security configuration settings for information technology products employed in AIS.

This *IT Security Handbook* and referenced policy and process documents address each of the CM controls as noted in Table 4-9.

**Table 4-9 Configuration Management Controls**

<b>Configuration Management Controls</b>				
<b>Control Number</b>	<b>Control Name</b>	<b>Control Baselines</b>		
		<b>Low</b>	<b>Moderate</b>	<b>High</b>
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	CM-2	CM-2 (1)	CM-2 (1) (2)
CM-3	Configuration Change Control	Not Selected	CM-3	CM-3 (1)
CM-4	Monitoring Configuration Changes	Not Selected	CM-4	CM-4
CM-5	Access Restrictions for Change	Not Selected	CM-5	CM-5 (1)
CM-6	Configuration Settings	CM-6	CM-6	CM-6 (1)
CM-7	Least Functionality	Not Selected	CM-7	CM-7 (1)
CM-8	Information System Component Inventory	CM-8	CM-8 (1)	CM-8 (1) (2)

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

## **4.9.2 Policy**

### **4.9.2.1 Configuration Management**

In accordance with *NIST SP 800-53, Rev. 1*, USPTO shall develop, disseminate, and periodically review/update: (i) a formal, documented, CM policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the CM policy and associated CM controls.

### **4.9.2.2 Baseline Configuration**

Each AIS shall have a current baseline configuration documented and maintained as required in the *Secure Baseline Policy*<sup>9</sup>. The secure baseline documents shall be periodically updated to reflect new security patches installed in accordance with the *Server Operating System Patch Management Procedures (IT-212.5-01:TN17)* and changes to industry best practices recommendations. Refer to the *Secure Baseline Policy* for additional policy and process guidance.

### **4.9.2.3 Configuration Change Control**

The USPTO shall authorize, document, and control change to all AIS. Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the AIS, including upgrades and modifications. Configuration change control includes changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers).

### **4.9.2.4 Monitoring Configuration Changes**

Each AIS shall be monitored for changes through conducting security impact analyses to determine the effects of changes to the system. Prior to change implementation, and as part of the change approval process, AIS changes shall be analyzed for potential security impacts. After the AIS is changed, including upgrades and modifications, the modified security features shall be verified to ensure proper function.

### **4.9.2.5 Access Restrictions for Change**

For moderate- and high-sensitivity AIS, each business area shall (i) approve individual access privileges and enforce physical and logical access restrictions associated with changes to the AIS; and (ii) generate, retain, and review records reflecting all such changes.

---

<sup>9</sup> Currently, the *Secure Baseline Policy* is in draft format.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

#### **4.9.2.6 Configuration Settings**

Each AIS shall have (i) an established mandatory configuration; (ii) the security settings of information technology products configured to the most restrictive mode consistent with AIS operational and business requirements; (iii) the configuration settings documented; and (iv) the configuration settings enforced in all AIS components. Refer to the *Secure Baseline Policy* for additional policy and process guidance.

#### **4.9.2.7 Least Functionality**

Each moderate- and high-sensitivity AIS shall be configured to provide only essential capabilities and specifically prohibit and/or restrict the use of specific functions, ports, protocols, and/or services as noted in the SSP or the operating system baseline configuration documentation.

#### **4.9.2.8 Information System Component Inventory**

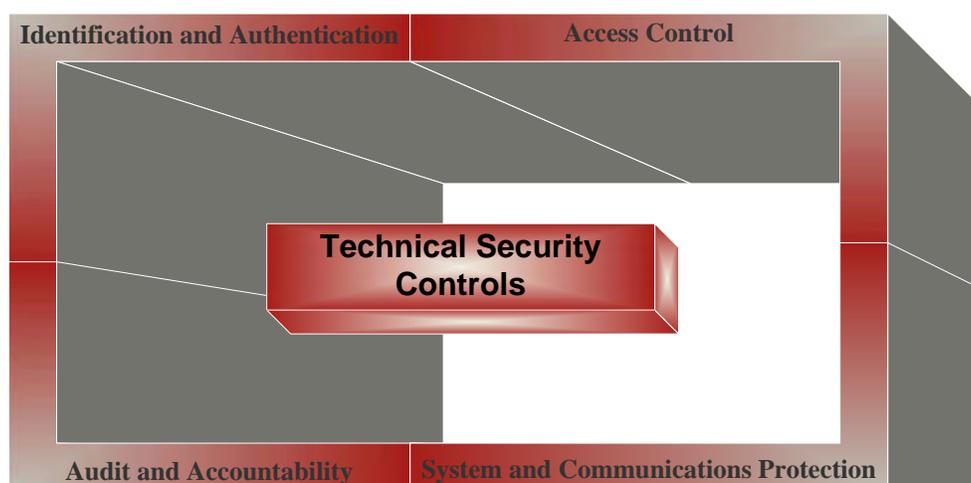
The USPTO shall develop, document, and maintain a current inventory of the AIS components and ownership information. Furthermore, each moderate- and high-sensitivity AIS shall update the inventory of AIS components as part of component installations and employ automated or manual mechanisms to help maintain a current, accurate, and available inventory.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

## **5 TECHNICAL CONTROLS**

Technical controls are those safeguards and countermeasures (typically described as security mechanisms) employed within the information system's hardware, software, or firmware to protect the system and its information from unauthorized access, use, disclosure, disruption, modification, or destruction. There are four (4) families within the technical class of security controls.

- Identification and Authentication
- Access Control
- Audit and Accountability
- System and Communications Protection



**Figure 5-1: Technical Security Controls**

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

## 5.1 Identification and Authentication

### 5.1.1 Purpose/Requirements

This technical control ensures that USPTO identifies AIS users, processes acting on behalf of users or devices, and authenticates (or verifies) the identities of those users, processes, or devices, as a prerequisite to allowing access to an AIS.

Providing access controls (identification) and authentication (validation of identity) is critical for protecting the confidentiality and preserving the integrity of electronic records. It is required to prevent unauthorized viewing, modification, destruction and, generally, the unauthorized issuance of commands.

User Identification (User ID) is used to identify persons working on an AIS. There are two forms of identification and authentication (I&A) used at the USPTO. The first is the typical User ID and password combination, known as a single factor I&A. In this form of I&A, access is granted based on unique knowledge traceable to an individual. Reference Remote Access Policy

The second form of I&A, called two-factor, is for highly sensitive applications, as well as situations where a password can be easily compromised or discovered, such as across the Internet. USPTO uses two different two-factor I&A systems: SecurID, a hardware token-based system, and X.509 digital certificates.

The *USPTO IT Security Handbook* and referenced policy and process documents address each of the Identification and Authentication controls as noted in Table 5-1.

**Table 5-1 Identification and Authentication Controls**

Identification and Authentication Controls				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
IA-1	Identification and Authentication Policy and Procedures	IA-1	IA-1	IA-1
IA-2	User Identification and Authentication	IA-2	IA-2 (1)	IA-2 (2) (3)
IA-3	Device Identification and Authentication	Not Selected	IA-3	IA-3
IA-4	Identifier Management	IA-4	IA-4	IA-4
IA-5	Authenticator Management	IA-5	IA-5	IA-5
IA-6	Authenticator Feedback	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	IA-7	IA-7	IA-7

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

## **5.1.2 Policy**

### **5.1.2.1 Identification and Authentication**

In accordance with *NIST SP 800-53, Rev.1*, the USPTO shall develop, disseminate, and periodically review/update: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

### **5.1.2.2 User Identification and Authentication**

All AIS shall be configured to uniquely identify and authenticate users. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or, in the case of multifactor authentication, some combination thereof. For moderate- and high- sensitivity AIS, multifactor authentication shall be compliant with *NIST SP 800-63, Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology*. Refer to *OMB Memorandum 04-04, E-Authentication Guidance* for additional policy and process guidance.

### **5.1.2.3 Device Identification and Authentication**

Each AIS shall identify and authenticate specific devices before establishing a connection.

**NOTE:** Public-facing web servers are exempt from this policy, as they do not require identification and authentication to establish a connection.

### **5.1.2.4 Identifier Management**

Each AIS shall manage user identifiers by (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate agency official; (iv) ensuring the user identifier is issued to the intended party; (v) disabling the user identifier after a reasonable period of inactivity; and (vi) archiving user identifiers.

### **5.1.2.5 Authenticator Management and Feedback**

AIS authenticators shall be managed by (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon AIS installation; and (iv) changing/refreshing authenticators periodically. Furthermore, the USPTO shall ensure that AIS obscure feedback of authentication information during the authentication process to protect the information from possible exploitation or use by unauthorized individuals. Electronic authentication methods to provide services must comply with *OMB Memorandum 04-04, E-Authentication Guidance*, and associated implementation requirements in *NIST SP 800-63*,

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

*Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology.*

### **5.1.2.6 Cryptographic Module Authentication**

Authentication methods shall be employed that meet the requirements of applicable laws, regulations, standards, and guidance for authentication to a cryptographic module. All AIS shall employ authentication methods that meet the requirements of *FIPS 140-2, Security Requirements for Cryptographic Modules*. FIPS approved encryption algorithms include:

- Advanced Encryption Algorithm (AES)
- Triple Data Encryption Algorithm (TDEA)

## **5.2 Access Control**

### **5.2.1 Purpose/Requirements**

This technical control ensures that USPTO identifies AIS users, processes acting on behalf of users or devices, and authenticates (or verifies) the identities of those users, processes, or devices, as a prerequisite to allowing access to an AIS.

Limiting system access to authorized users is an essential part of good computer security and is done in several ways. First, access is controlled through the use of a User ID/Password combination. If an employee does not have a valid User ID and Password, the employee is denied access to USPTO systems.

Second, employee permissions or privileges are limited to only those necessary to perform specific responsibilities. This principle is called “least privilege” and is implemented by assigning appropriate rights or privileges to each User ID/Password combination. The rights assigned to employees are determined by the job performed and the permissions requested and approved by the appropriate supervisor. Supervisors, Contracting Officers, and Contracting Officer’s Technical Representatives (COTRs) shall continuously assess the privileges granted to employees and contractors and submit the necessary requests to change or remove access to those systems and network resources that are no longer required.

Finally, access to the network may be controlled through the use of specific devices designed to limit connections to the network and computer resources. For example, the agency employs firewalls and routers in the network infrastructure that can be used to restrict traffic into and out of the network.

The *USPTO IT Security Handbook* and referenced policy and process documents address each of the Access Controls as noted in Table 5-2 on the next page.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

**Table 5-2 Access Controls**

<b>Access Controls</b>				
<b>Control Number</b>	<b>Control Name</b>	<b>Control Baselines</b>		
		<b>Low</b>	<b>Moderate</b>	<b>High</b>
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	AC-3	AC-3 (1)	AC-3 (1)
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	Not Selected	AC-5	AC-5
AC-6	Least Privilege	Not Selected	AC-6	AC-6
AC-7	Unsuccessful Login Attempts	AC-7	AC-7	AC-7
AC-8	System Use Notification	AC-8	AC-8	AC-8
AC-11	Session Lock	Not Selected	AC-11	AC-11
AC-12	Session Termination	Not Selected	AC-12	AC-12 (1)
AC-13	Supervision and Review—Access Control	AC-13	AC-13 (1)	AC-13 (1)
AC-14	Permitted Actions without Identification or Authentication	AC-14	AC-14 (1)	AC-14 (1)
AC-17	Remote Access	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access Restrictions	AC-18	AC-18 (1)	AC-18 (1) (2)
AC-19	Access Control for Portable and Mobile Devices	Not Selected	AC-19	AC-19
AC-20	Use of External Information Systems	AC-20	AC-20 (1)	AC-20 (1)

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

## **5.2.2 Policy**

### **5.2.2.1 Access Control**

In accordance with *NIST SP 800-53, Rev.1*, USPTO shall develop, disseminate, and periodically review/update: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

To establish a PTONet account, the USPTO supervisor shall request a network account and password for the USPTO staff member, in writing. Additional requirements include:

- Employees cannot have more than one system or network user account, unless their position or the functions of their position require them to have multiple accounts. For example, a System Administrator would have two accounts: an administrator account used when performing system administration functions, and a user account for routine use.
- USPTO does not permit the use of accounts named “group,” “guest,” “student,” or “test.” and default accounts used by software packages.
- Employees are not permitted to use a group account that would be shared with co-workers. **NOTE:** Systems located within a datacenter may share accounts at the console level. Refer to the *Password Management Policy* for additional policy and process guidance.
- All USPTO workstations shall use password-protected screen savers as documented in the *Password Protected Screen Saver Policy*. Employees are NOT authorized to download or install screen savers. Screen savers shall be selected from a list of authorized operating system manufacturer default screen savers selected for optimum performance to ensure low system resource utilization, (i.e., memory and CPU resource utilization), prevent potential introduction of malicious code, and ensure that screen savers do not adversely impact applications employees use.
- There are no limitations or restrictions on access to the Internet for business purposes. If employees are using the Internet for other than business purposes, employees must comply with the *Rules of the Road*.
- The use of Internet services such as streaming audio and video, chat rooms, and instant messaging is authorized, if necessary, for business purposes. Personal use of these services is restricted and governed by the *Limited Personal Use Policy* and the *Rules of the Road*.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- Employees are not authorized to download, install or run/execute scripts, macros, utilities, screen savers, applications or other executable software without receiving approval through the *Software Product Approval Process*.

### **5.2.2.2 Account Management**

All AIS accounts shall be managed, including establishing, activating, modifying, reviewing, disabling, and removing accounts. AIS accounts shall be reviewed in accordance with system requirements. Each moderate- and high-sensitivity AIS shall (i) employ automated mechanisms to support the management of AIS accounts; (ii) terminate temporary and emergency accounts after a reasonable period of time for each type of account; (iii) disable inactive accounts after 90 days; and, (iv) The USPTO Enterprise Asset Management System (EAMS) shall be employed to ensure that account creation, modification, disabling, and termination actions are audited and to notify, as required, appropriate individuals.

### **5.2.2.3 Access Enforcement**

All AIS shall enforce assigned authorizations for controlling access to the system in accordance with the SSP. For moderate- and high-sensitivity AIS, access is restricted to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

### **5.2.2.4 Information Flow Enforcement**

All AIS shall enforce assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with the SSP.

### **5.2.2.5 Separation of Duties**

The principle of separation of duties ensures that no single individual has total control of the system's security mechanisms, and, therefore, no one individual can compromise the system completely. To ensure separation of duties, each moderate- and high-sensitivity AIS shall adhere to the following guidance:

- System security-related tasks shall be apportioned to several individuals.
- The security principle of least privilege shall be applied to all systems.
- Users and processes in a system shall have the least number of privileges for the least amount of time required to perform assigned tasks.

Execution of logical access control security functions shall follow the practice of separation of duties. Separation of duties requires the segregation of logical access control security, programming, database administration, user, and other IT functions into separate job functions performed by different individuals.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

#### **5.2.2.6 Least Privilege**

All AIS shall operate in such a way that they run with the least amount of system privilege needed to perform a specific function and that system access is granted on a need-to-know basis. As a result, logical access controls shall be based on the principle of least privilege, which means that users will be granted access to the minimum resources required to perform their official job functions.

#### **5.2.2.7 Automatic Account Lockout**

Where feasible, account lockout controls shall be implemented and enforced to limit the number of consecutive failed log-on attempts against a given AIS. After the mandatory lockout period, users should contact the USPTO Help Desk if they have problems logging back on. Refer to the *Password Management Policy* for additional policy and process guidance.

#### **5.2.2.8 System Use Notification**

All USPTO business areas shall ensure that AIS and networks display USPTO-approved warning banners for all access points. Employees and contractor employees, or any person who accesses an AIS will be notified on entry through a warning banner that must be agreed to, prior to being allowed to proceed with log-on. Where feasible, IT systems will display the USPTO-approved log-on warning banner. Warning banners shall describe the authorized use of systems and include clauses on user expectations of privacy and user consent to monitoring.

This warning banner shall state that all AIS may be monitored and that unauthorized use will be grounds for disciplinary, civil or criminal proceedings. Refer to the *Rules of the Road* for a sample of the USPTO log-on banner.

#### **5.2.2.9 Automatic Session Lockout**

Refer to the *Password Protected Screen Saver Policy* and the *Remote Access Policy* for specific policy and process guidance.

#### **5.2.2.10 Session Termination**

All moderate- and high-sensitivity AIS shall automatically terminate remote sessions in accordance with the *Remote Access Policy*. Remote or local sessions that use root or administrator access shall terminate after 60 minutes of inactivity.

#### **5.2.2.11 Supervision and Review**

User activities, with respect to the enforcement and usage of AIS access controls, shall be supervised and enforced. For moderate- and high-sensitivity AIS, mechanisms shall be in place to facilitate the review of user activities.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

#### **5.2.2.12 Permitted Actions without Identification and Authentication**

Access to an AIS shall not be granted without identification or authentication, unless a waiver has been approved or if it is a public web server being accessed in an authorized and legal manner

#### **5.2.2.13 Remote Access**

All AIS shall authorize, monitor, and control all methods of remote access. Each moderate- and high-sensitivity AIS shall:

- Employ automated mechanisms to facilitate the monitoring and control of remote access;
- Use cryptography to protect the confidentiality and integrity of remote access sessions; and
- Document the rationale for such access in the AIS SP.

USPTO categorizes remote access into three tiers, according to the risk of harm inherent in the nature of the access and the sensitivity of the information accessed.

- Tier 1 represents low risk since the AIS accessed are between the outermost USPTO network perimeter or border device, such as the USPTO firewall, and outside inner USPTO firewalls that protect local area networks. Tier 1 information is of low sensitivity.
- Tier 2 represents medium risk since basic user privileges are allowed to access AIS processing or storing *Sensitive But Unclassified* information inside the inner USPTO firewalls and internal to the USPTO computing environment.
- Tier 3 represents high risk since administrative (or “super-user”) privileges are allowed to access AIS processing or storing *Sensitive But Unclassified* information that are internal to the USPTO computing environment.

Refer to the *Remote Access Policy* for additional policy and process guidance.

#### **5.2.2.14 Wireless Access**

The USPTO shall (i) establish usage restrictions and implementation guidance for wireless technologies; and (ii) authorize, monitor, and control wireless access to an AIS.

Wireless networks or systems are not permitted in the USPTO without the written approval of the USPTO CIO. For all approved wireless networks that access a moderate or high sensitivity AIS, authentication and encryption shall be employed to protect wireless access. Proposals for the use of wireless devices for processing official information must be submitted to the OCIO IT Security Program Office Director. If a USPTO Office is considering the use of wireless

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

technology, the Office must contact the OCIO Business Relationship Management Group (BRMG) for consultation and assistance. BRMG will coordinate CIO review of the proposal.

The following procedures shall be used to request a wireless system:

1. The manager of any USPTO Office considering the use of wireless technology in the USPTO must first contact the OCIO BRMG.
2. BRMG will assign an account manager that will coordinate with the technical lead in the requesting USPTO Office and with appropriate OCIO staff.
3. The technical leads from both offices will prepare a business case for the wireless technology that will address the following:
  - Requirement to be met with the wireless technology
  - Reason why wireless was the chosen technology to be applied
  - How IT Security safeguards will be incorporated into the solution selected
  - The number and types of users of the wireless solution.
4. The technical leads will provide the business case to BRMG for review.
5. BRMG will coordinate review of the business case, obtain a decision, and report the decision back to the requestor.
6. If approved, the wireless proposal will be assigned to PMO, who will follow SDLC procedures to implement the solution.

#### **5.2.2.15 Access Control for Portable and Mobile Devices**

Portable and mobile devices shall not be connected to a non-USPTO network and the USPTO network at the same time. Automated vulnerability and compliance scanning shall be executed against portable and mobile computing systems accessing USPTO AISs remotely.

When traveling with a portable computer, employees shall take the necessary precautions to ensure that the computer is not left unattended or unsecured. Employees shall back up information prior to departure on travel and regularly under other conditions, to protect the information on the computer from loss. Sensitive data, including personally identifiable information, shall not be stored on portable computers unless they are encrypted. Refer to the *IT Privacy Policy* and the *Remote Access Policy* for additional policy and process guidance.

Physical access shall be controlled for portable and mobile AIS (e.g., laptops) accessing or containing business and mission critical AIS and information (e.g., records maintained of authorized use, encryption used as necessary).

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

### **5.2.2.16 Use of External Information Systems**

For moderate- and high-sensitivity AIS, authorized individuals shall be prohibited from using an external AIS to access the AIS or to process, store, or transmit organization-controlled information except in situations where the organization: (i) can verify the employment of required security controls on the external system as specified in the organization’s information security policy and SSP; or (ii) has approved AIS connection or processing agreements with the organizational entity hosting the external AIS. Refer to the Remote Access Policy for more details.

## **5.3 Audit and Accountability**

### **5.3.1 Purpose/Requirements**

This technical control ensures that USPTO (i) creates, protects, and retains AIS audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate AIS activity; and (ii) ensures that the actions of individual AIS users can be uniquely traced to those users so they can be held accountable for their actions.

The *USPTO IT Security Handbook* and referenced policy and process documents address each of the Audit and Accountability controls as noted in Table 5-3.

**Table 5-3 Audit and Accountability Controls**

<b>Audit and Accountability Controls</b>				
<b>Control Number</b>	<b>Control Name</b>	<b>Control Baselines</b>		
		<b>Low</b>	<b>Moderate</b>	<b>High</b>
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU-1	AU-1
AU-2	Auditable Events	AU-2	AU-2 (3)	AU-2 (1) (2) (3)
AU-3	Content of Audit Records	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Monitoring, Analysis, and Reporting	Not Selected	AU-6 (2)	AU-6 (1) (2)
AU-7	Audit Reduction and Report Generation	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	AU-9	AU-9	AU-9
AU-11	Audit Record Retention	AU-11	AU-11	AU-11

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

## **5.3.2 Policy**

### **5.3.2.1 Audit and Accountability**

In accordance with *NIST SP 800-53, Rev.1*, the USPTO shall develop, disseminate, and periodically review/update: (i) a formal documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

### **5.3.2.2 Auditable Events**

All AIS shall document what audit events shall be included in the SSP. Furthermore, each moderate- and high-sensitivity AIS shall be periodically reviewed and the USPTO-defined auditable events updated.

An audit trail shall include sufficient information to establish what activity occurred and who (or what) caused them. The scope and contents of the audit trail shall balance security needs with performance needs, privacy, and costs. Refer to the *Network and AIS Audit Logging Policy* for additional policy and process guidance.

### **5.3.2.3 Audit Storage Capacity**

All AIS shall contain sufficient audit record storage capacity and configure auditing to reduce the likelihood of such capacity being exceeded.

### **5.3.2.4 Response to Audit Processing Failures**

Each AIS shall alert appropriate organizational officials in the event of an audit processing failure. Refer to the *Network and AIS Audit Logging Policy* for additional policy and process guidance.

### **5.3.2.5 Audit Monitoring, Analysis, and Reporting**

AIS audit records shall be regularly reviewed and analyzed for indications of inappropriate or unusual activity, suspicious activity or suspected violations investigated, findings reported to appropriate officials, and necessary actions taken. Furthermore, moderate- and high-sensitivity AIS shall contain automated mechanisms to alert security personnel of inappropriate or unusual activities with security implications. Refer to the *Network and AIS Audit Logging Policy* for additional policy and process guidance.

### **5.3.2.6 Audit Reduction and Report Generation**

AIS shall provide an audit reduction and report generation capability based on specific event criteria. Each moderate- and high-sensitivity AIS shall provide the capability to automatically

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

process audit records for events based upon event criteria. Refer to the *Network and AIS Audit Logging Policy* for additional policy and process guidance.

### **5.3.2.7 Time Stamps**

AIS shall provide time stamps for use in audit record generation. Refer to the *Network and AIS Audit Logging Policy* for additional policy and process guidance.

### **5.3.2.8 Protection of Audit Information**

The AIS shall protect audit information and audit tools from unauthorized access, modification, and deletion. Refer to the *Network and AIS Audit Logging Policy* for additional policy and process guidance.

### **5.3.2.9 Audit Record Retention**

Refer to the *Network and AIS Audit Logging Policy* for audit record retention policy and process guidance.

## **5.4 System and Communications Protection**

### **5.4.1 Purpose/Requirements**

This technical control ensures that the USPTO (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by agency AIS) at the external boundaries and key internal boundaries of AIS; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within agency AIS.

The *USPTO IT Security Handbook* and referenced policy and process documents address each of the System and Communications Protection controls as noted in Table 5-4.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

**Table 5-4 System and Communications Protection Controls**

<b>System and Communications Protection Controls</b>				
<b>Control Number</b>	<b>Control Name</b>	<b>Control Baselines</b>		
		<b>Low</b>	<b>Moderate</b>	<b>High</b>
SC-1	System and Communications Protection Policy and Procedures	SC-1	SC-1	SC-1
SC-2	Application Partitioning	Not Selected	SC-2	SC-2
SC-4	Information Remnance	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	SC-5	SC-5	SC-5
SC-7	Boundary Protection	SC-7	SC-7 (1) (2) (3) (4)	SC-7 (1) (2) (3) (4) (5) (6)
SC-8	Transmission Integrity	Not Selected	SC-8	SC-8 (1)
SC-9	Transmission Confidentiality	Not Selected	SC-9	SC-9 (1)
SC-10	Network Disconnect	Not Selected	SC-10	SC-10
SC-12	Cryptographic Key Establishment and Management	Not Selected	SC-12	SC-12
SC-13	Use of Cryptography	SC-13	SC-13	SC-13
SC-14	Public Access Protections	SC-14	SC-14	SC-14
SC-15	Collaborative Computing	Not Selected	SC-15	SC-15
SC-17	Public Key Infrastructure Certificates	Not Selected	SC-17	SC-17
SC-18	Mobile Code	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	Not Selected	SC-19	SC-19
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	Not Selected	SC-20	SC-20
SC-22	Architecture and Provisioning for Name/Address Resolution Service	Not Selected	SC-22	SC-22
SC-23	Session Authenticity	Not Selected	SC-23	SC-23

## **5.4.2 Policy**

### **5.4.2.1 System and Communications Protection**

In accordance with *NIST SP 800-53, Rev.1*, the USPTO shall develop, disseminate, and periodically review/update: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

#### **5.4.2.2 Application Partitioning**

Each AIS shall separate user functionality (including user interface services) from AIS management functionality.

#### **5.4.2.3 Information Remnance**

Each AIS shall prevent unauthorized and unintended information transfer via shared system resources.

#### **5.4.2.4 Denial of Service Protection**

Each AIS shall protect against or limit the effects of denial of service attacks, as documented in the SSP or the common controls SSP.

#### **5.4.2.5 Boundary Protection**

Each AIS shall monitor and control communications at the external boundary of the AIS and at key internal boundaries within the system. Furthermore, each moderate- and high-sensitivity AIS shall (i) physically allocate publicly accessible AIS components to separate sub-networks with separate, physical network interfaces; (ii) prevent public access into the Agency's internal networks except as appropriately mediated; (iii) limit the number of access points to the AIS to allow for better monitoring of inbound and outbound network traffic; (iv) implement a managed interface (boundary protection devices in an effective security architecture) with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted, (v) deny network traffic by default and allow network traffic by exception (i.e., deny all, permit by exception); and (vi) prevent the unauthorized release of information outside of the AIS boundary or any unauthorized communication through the boundary when there is an operational failure of the boundary protection mechanisms.

#### **5.4.2.6 Transmission Integrity and Confidentiality**

All moderate- and high-sensitivity AIS shall protect the integrity and confidentiality of transmitted information through the use of cryptographic mechanisms that recognize changes to information during transmission and prevents the unauthorized disclosure of information during transmission.

#### **5.4.2.7 Network Disconnect**

Each AIS shall terminate a network connection at the end of a session or after a reasonable period of inactivity and document that period in the system security plan.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

#### **5.4.2.8 Cryptographic Key Establishment and Management**

When cryptography is required and employed within moderate- and high-sensitivity AIS, the System Administrator shall establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures. For information that requires cryptographic protection, all AIS shall employ authentication methods that meet the requirements of *FIPS 140-2, Security Requirements for Cryptographic Modules*. FIPS approved encryption algorithms include:

- AES
- TDEA (3DES)

#### **5.4.2.9 Public Access Protections**

For publicly available systems, SOs shall ensure that AIS protect the integrity of the information and applications residing on the system.

#### **5.4.2.10 Collaborative Computing**

Each moderate- and high-sensitivity AIS shall prohibit remote activation of collaborative computing mechanisms and provide an explicit indication of use to the local users.

#### **5.4.2.11 Public Key Infrastructure**

Public Key Infrastructure (PKI) includes security services supporting digital signatures and encryption. Digital certificates, and policies and procedures surrounding their issuance, provide for authentication of data and verification that the person signing the document is who he or she claims to be.

A PKI is the sum total of the hardware, software, people, processes, and policies that, together, using the technology of asymmetric cryptography, facilitate the creation of a verifiable association between a public key (the public component of an asymmetric key pair) and the identity (and/or other attributes) of the holder of the corresponding private key (the private component of that pair). A PKI uses the verifiable association between the public and private keys to authenticate the identity of a specific entity, ensure the integrity of information, provide support for non-repudiation, and establish encrypted communication sessions.

Any cryptographic keys and digital certificates used by the PKI shall be protected with passwords that adhere to the *Password Management Policy*.

The USPTO shall issue public key certificates under an appropriate certificate policy or obtain public key certificates under an appropriate certificate policy from an approved service provider. For user certificates, the USPTO shall establish an agency certification authority cross-certified with the Federal Bridge Certification Authority at medium assurance or higher or use certificates from an approved, shared service provider, as required by *OMB Memorandum 05-24. The*

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

*USPTO shall maintain Certificate Policy and Certificate Practices Statement that are RFC3647 compliant; further PKI-related policies may be found in those documents.*

#### **5.4.2.12 Mobile Code**

Each AIS shall (i) establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the AIS if used maliciously; and (ii) authorize, monitor, and control the use of mobile code within the AIS. Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript.

USPTO employees and contractor employees shall preserve standard configuration settings on applications that restrict automatic mobile code execution. Where mobile code is necessary for a system implementation, the SO shall pursue CIO approval via the ITSMG waiver process.

#### **5.4.2.13 Communications Security (Voice/Data (Facsimile/VoIP))**

The USPTO shall (i) establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the AIS if used maliciously; and (ii) authorize, monitor, and control the use of VoIP within the AIS.

To ensure that adequate communications security is in place for voice, data, facsimile, and VoIP, the following guidelines shall be followed:

- USPTO staff may only connect an OCIO-approved personal digital assistant (PDA) to a computer connected to the USPTO network for file/data/e-mail/calendar exchange and synchronization purposes.
- USPTO staff must adhere to ITSMG specific instructions regarding the use of PDAs and the protection requirements for sensitive data stored on PDAs. Refer to the *IT Privacy Policy* for additional policy and process guidance.
- When information that should not be releasable to the general public is transferred from one system to another, the confidentiality or disclosure of the information must be protected using secure transfer mechanisms listed in this document and other applicable USPTO policies.
- Workstations shall use an approved, configuration-controlled, commercially available browser to access Internet web sites. Browsers are kept current with the latest security patches and fixes, and the use of some browser features may be restricted. Any restrictions necessary for security or other reasons are detailed in this document and other applicable USPTO policies.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

#### **5.4.2.14 Secure Name/Address Resolution Service (Authoritative Source)**

Each AIS shall provide name/address resolution service and additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries. This control enables remote clients to obtain origin authentication and integrity verification assurances for the name/address resolution information obtained through the service. A domain name system (DNS) server is an example of an AIS that provides name/address resolution service; digital signatures and cryptographic keys are examples of additional artifacts  
Architecture and Provisioning for Name/Address Resolution Service.

For moderate- and high-sensitivity AIS that collectively provide name/address resolution, the service shall be fault tolerant and implement role separation. A resolving or caching DNS server is an example of an AIS that provides name/address resolution service for local clients, and authoritative DNS servers are examples of authoritative sources.

#### **5.4.2.15 Session Authenticity**

Each AIS shall provide mechanisms to protect the authenticity of communications sessions. Refer to *NIST SP 800-77, Guide to IPsec VPNs*, and *NIST SP 800-95, Guide to Secure Web Services* for guidance specific to securing sessions.

This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.

## 6 POLICY ENFORCEMENT

Violation of policy may result in administrative or adverse action in accordance with OHR policies. Perceived threats to system integrity, confidentiality, or availability shall result in suspension of system access as necessary to contain the perceived threat. Offenses that are in violation of local, state, or Federal laws may result in suspension of system access and shall be reported to the appropriate law enforcement authorities.

What are the consequences if USPTO staff know of or observe an incident and do not report it?

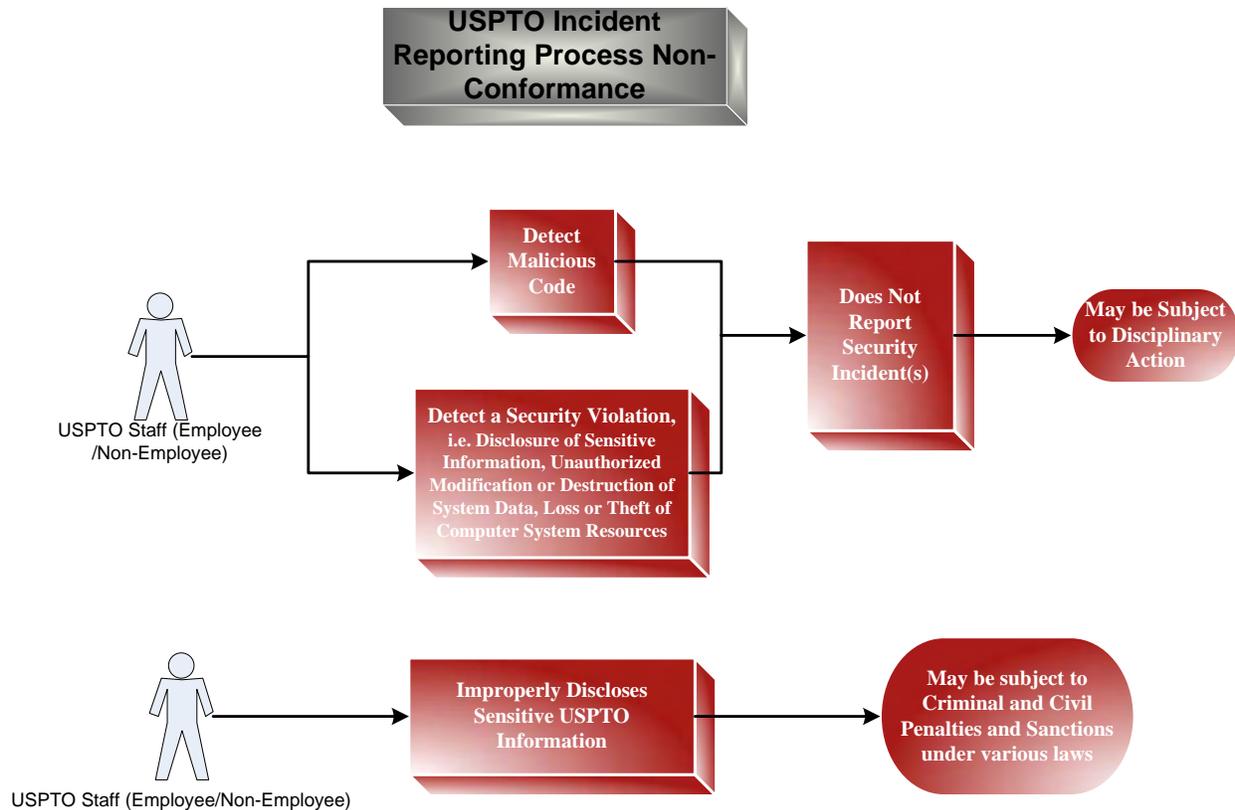


Figure 6-1: USPTO Incident Reporting Process Non-Conformance

USPTO IT security policies shall be enforced through the following:

- Oversight
- Inspection
- Audit
- Violation Action

COTRs have contract oversight security responsibilities and shall ensure that contractor-related security requirements are followed throughout the contract lifecycle.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

Refer to the *Discipline and Penalties Policy* for specific policy and process guidance.

## **6.1 Inspections**

The ITSMG shall design and conduct inspections of the various USPTO IT Security Programs, including the IT Security Training Program and evaluate their effectiveness.

These inspections shall examine:

- Effectiveness of security control measures
- Compliance with existing policies, procedures, standards and guidelines
- User community security and policy awareness
- Active adoption of this policy's requirements

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

## **7 WAIVERS**

Waivers to any of the USPTO IT security policies must be approved by the CIO or CISO. Waivers must be submitted in writing to the ITSMG for evaluation and recommendation. For tracking purposes, waiver requests shall be provided by e-mail to the “HELPDESK 9000” e-mail address. The USPTO Help Desk shall initiate a Change Request (CR) in the EAMS and assign the waiver request to appropriate ITSMG staff.

Temporary waiver requests of a general nature will not be considered. Requesting offices shall be notified when final waiver approval is granted, or if the waiver request is denied following the review period. If the waiver is denied, the requesting office shall coordinate with the ITSMG to resolve questions and/or issues regarding the request.

Any employee or contractor employee responsible for the management, implementation, installation, configuration, operation, maintenance, or security of an AIS shall identify proposed deviations from the mandatory practices of this policy and request a waiver in writing from the ITSMG. Approved waivers shall be documented as part of the appropriate SSP(s) that cover the system(s) applicable to the waiver. Identical systems under the same management authority and covered by one SSP require only one waiver request.

Requests for waivers shall include:

- Specific mandatory practice(s) for which the waiver is requested
- Rationale for the requested waiver
- If applicable, a description of compensating controls to be in place during the period of the requested waiver, until compliance is accomplished, and an action plan (including target dates) for compliance
- Management approval in writing

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

## **APPENDIX A REFERENCES**

The following list of Federal laws, regulations, and guidance provides the basis and additional guidance for the development of the *USPTO IT Security Handbook*.

- 5 U.S.C. 552a, 552a Note, *The Privacy Act of 1974*.
- 5 U.S.C. 552, 552 Notes, *Freedom of Information Act of 1974*.
- 44 U.S.C Chapter 31, *Records Management by Federal Agencies*.
- *Clinger-Cohen Act of 1996*, June 1997.
- *Control Objectives for Information and Related Technology (COBIT) 4th Edition*, IT Governance Institute, December 2005.
- Department of Defense Trusted Computer Systems Evaluation Criteria (TCSEC), DOD-5200.28-Std.
- E-Government Act (Public Law 107-347), Title III - *Federal Information Security Management Act (FISMA)*, December 2002.
- *Federal Financial Management Improvement Act of 1996*, September 1996.
- Federal Information Processing Standards (FIPS) Publication 140-2, *Security requirements for Cryptographic Modules*, May 2001.
- Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
- Federal Information Processing Standard (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.
- General Accounting Office (GAO), *Standards for Internal Control in the Federal Government*, November 1999.
- GAO, *Federal Information System Controls Audit Manual (FISCAM)*, January 1999
- GAO, *Government Auditing Standards*, July 1996.
- *Government Paperwork Elimination Act*, October 1998.
- Homeland Security Presidential Decision Directive/HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.
- *Information Technology Management Reform Act of 1996* (Public Law 107-347), August 1996.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- ISSO 17799, *A Code of Practice for Information Security Management* (British Standard 7799).
- NIST “*Common Criteria for Information Technology Security Evaluation,*” Version 2.1 (CC 2.1), August 1999.
- NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.
- NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology*, June 1996.
- NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Base Model*, April 1998.
- NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998.
- NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.
- NIST SP 800-34, *Contingency Planning Guide for IT Technology Systems*, June 2002.
- NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.
- NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, September 2002.
- NIST SP 800-53, Rev. 1, *Recommended Security Controls for Federal Information Systems*, December 2006.
- NIST SP 800-53, Rev. 1, *Recommended Security Controls for Federal Information Systems*, December 2006, Annex 1, Annex 2, Annex 3 (updates through 6/17/05).
- NIST SP 800-53A, SPD, *Guide for Assessing the security Controls in Federal Information System*, April 2006.
- NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.
- NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*, October 2003.
- Office of Management and Budget (OMB) Circular A-127, *Financial Management Systems*, July 23, 1993.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, Appendix III, Revised November 2000.
- OMB Memorandum 99-05, *Instructions on Complying with the President's Memorandum of May 14, 1998--Privacy and Personal Information in Federal Records*, July 1, 1999.
- OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 17, 2001.
- OMB Memorandum M-02-09, *Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones*, July 2, 2002.
- OMB Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act*, August 6, 2003.
- OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 30, 2003.
- OMB Memorandum 04-04, *E-Authentication Guidance*, December 16, 2003.
- OMB Memorandum 04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*, August 23, 2004.
- OMB Memorandum 04-26, *Personal Use Policies and "File Sharing" Technology*, September 8, 2004.
- OMB Memorandum 06-15, *Safeguarding Personally Identifiable Information*, May 22, 2006.
- OMB Memorandum 06-16, *Protection of Sensitive Agency Information*, June 23, 2006.
- OMB Memorandum 06-19, *Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments*, July 12, 2006.
- OMB Memorandum 06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, July 17, 2006.
- *Paperwork Reduction Act of 1995*, October 1995.
- *Paperwork Reduction Reauthorization Act of 1986*, October 1986.
- Public Law 100-235, *Computer Security Act of 1987*, January 8, 1988.

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

- U.S. Department of Commerce, *IT Security Program Policy and Minimum Implementation Standards*, June 30, 2005.
- United States Patent and Trademark Office, 5 CFR, Part 930.302, *USPTO Training Requirements*.
- NIST SP 800-61, Rev. 1, *Computer Security Incident Handling Guide*, September 2007

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

## **APPENDIX B ACRONYMS AND ABBREVIATIONS**

<b>Acronym</b>	<b>Meaning</b>
AAO	Agency Administrative Order
AES	Advanced Encryption Algorithm
AETS	Architecture, Engineering, and Technical Services
AIS	Automated Information System
AO	Authorizing Official
API	Application Program Interface
ATO	Authority to Operate (Full Accreditation)
BC/DR	Business Continuity/Disaster Recovery
BRM	Business Reference Model
BRMG	Business Relationship Management Group
C&A	Certification and Accreditation
CA	Certification Agent
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CM	Configuration Management
CO	Certifying Official
COOP	Continuity of Operations
COTR	Contracting Officer's Technical Representatives
CP	Contingency Plan
CR	Change Request
CT	Certification Testing
CTP	Certification Test Plan
CTR	Certification Test Report
DATO	Deny Authorization to Operate

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

Acronym	Meaning
DHS	Department of Homeland Security
DNS	Domain Name System
DOC	Department of Commerce
DOD	Department of Defense
EA	Enterprise Architecture
ESA	Enterprise Security Architecture
EVM	Earned Value Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
GAO	Government Accounting Office
GSA	General Services Administration
GSS	General Support System
HSPD	Homeland Security Presidential Directive
I&A	Identification and Authentication
IATO	Interim Authority to Operate (Interim Accreditation)
IDS	Intrusion Detection Systems
ITIRB	Information Technology Investment Review Board
IRM	Information Resources Management
ISA	Interconnection Security Agreement
ISSO	Information System Security Officer
IT	Information Technology
ITIM	Information Technology Investment Management
ITSMG	Information Technology Security Policy Division
ITTB	Information Technology Testing Branch
LAN	Local Area Network

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

Acronym	Meaning
LMS	Learning Management System
MA	Major Application
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NAC	National Agency Check
NACI	National Agency Check with Investigation
NSA	National Security Agency
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OGC	Office of General Counsel
OHR	Office of Human Resources
OIG	Office of Inspector General
OMB	Office of Management and Budget
OSP	Operational Support Plan
PDA	Personal Digital Assistant
PIA	Privacy Impact Assessment
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PMO	Program Management Office
POA&M	Plan of Action and Milestones
POC	Point of Contact
PM	Project Manager
PRA	Preliminary Risk Assessment
PTONet	USPTO network
RA	Risk Assessment

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

Acronym	Meaning
RTM	Requirements Traceability Matrix
SAISO	Senior Agency Information Security Officer
SAP	Security Accreditation Package
SC	Security Categorization
SCAD	Security Controls Assessment Determination
SDLC	System Development Life Cycle
SDL	System Development Lead
SO	System Owner
SP	Special Publication
SSP	System Security Plan
ST&E	Security Test and Evaluation
TDEA	Triple Data Encryption Algorithm
TN	Technical Note
TVA	Technical Vulnerability Assessments
UPS	Uninterruptible Power Supply
US-CERT	United States Computer Emergency Readiness Team
User ID	User Identification
USPTO	United States Patent and Trademark Office
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

## **APPENDIX C GLOSSARY**

<b>Term</b>	<b>Definition</b>
Acceptable Level of Risk	A judicious, carefully considered, and fully documented assessment by the appropriate Designated Approving Authority (AO) that an AIS meets the minimum requirements of applicable security directives. The assessment should take into account and carefully document the sensitivity and criticality of information, threats, vulnerabilities and countermeasures and their effectiveness in compensating for vulnerabilities, and operational requirements.
Acceptable Risk	A concern that is deemed acceptable to responsible management, due to the cost and magnitude of implementing countermeasures to mitigate the risk.
Accountability:	Accountability is (1) The quality or state that enables violations or attempted violations of IT Security to be traced to individuals who may then be held responsible. (2) The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, after-action recovery and legal action.
Accreditation	(1) The procedure for accepting an information technology (IT) system to process sensitive information within a particular operational environment. (2) Formal declaration by a Designated Approving Authority (AO) that an information system is approved to operate in a particular security configuration using a prescribed set of safeguards. (3) The managerial authorization and approval granted to a system or network to process sensitive data in an operational environment. This authorization is made on the basis of a certification recommendation by designated technical personnel with extensive security expertise and direct knowledge of the system. This authorization is only granted if the design and implementation of the system meet pre-specified technical requirements for achieving adequate data security. (4) A formal declaration by the AO, based on the recommendation of the certifier, that the information system is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an AIS and is based on the certification process, the assessment and analysis of the certifier as well as other management considerations. The accreditation statement affixes security responsibility to the AO and shows that due care for security has been taken.
Active Content	Active content refers to electronic documents that can carry out or trigger actions automatically on a computer platform without the intervention of a user. Active content technologies allow mobile code associated with a document to execute as the document is rendered. Examples of active content include PostScript documents, Web pages containing Java applets and JavaScript instructions, proprietary desktop-application formatted files containing macros, spreadsheet formulas, or other interpretable content, interpreted electronic mail formats having embedded code or bearing executable attachments and ActiveX technology. Active content is also frequently, but not necessarily, associated with Mobile Code.
Accreditation Package	The evidence provided to the authorizing official to be used in the security accreditation decision process. Evidence includes, but is not limited to: (i)

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

<b>Term</b>	<b>Definition</b>
	the system security plan; (ii) the assessment results from the security certification; and (iii) the plan of action and milestones.
Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Application	The use of information resources (information and information technology) to satisfy a specific set of users requirements (See Major Application).
Assurance	Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. "Adequately met" includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software, and (3) sufficient resistance to intentional penetration pr bypass.
Audit Log	A chronological record of system activities which enables the reconstruction and examination of the sequence of events and activities surrounding or leading to an operation, a procedure or an event in a transaction from its inception to final results. The audit log also serves as the chain of custody for the history of use of a record. This term is synonymous with Audit Records and Audit Trails.
Authentication	The process of determining the identity of a user, device or other entity in a computer system, as a prerequisite to allowing access to resources in a system. Verification of a user's identity ensures that the person requesting access to the network is, in fact, the person to whom entry is authorized.
Authorized User	A member of the public, a USPTO employee, contractor or subcontractor with assigned, approved permissions and privileges to access the network. An authorized user has access to specific activities and resources on the network. Use beyond those authorized is a violation of policy and of the law.
Automated Information System (AIS)	A combination of functional users, information technology personnel, business processes and procedures, application software, system software, documentation, commercial off-the-shelf software, computer, networking and other information technology resources that collect, record, process, store, communicate, retrieve, display, and disseminate information.
Availability	Assurance that information, services, and AIS resources are accessible to authorized users and/or system-related processes on a timely and reliable basis and are protected from denial of service.
Certification	The technical evaluation that establishes the extent to which a computer system, application or network design and implementation meet a specified set of security requirements. See also Accreditation.
Chief Information Security Officer	See Senior Agency Information Security Officer.
Common Criteria	A multi-part standard (ISO/IEC 15408) that defines criteria to be used as the basis for evaluating security properties of information technology products and systems. By establishing such a common criteria base, the results of an information technology security evaluation are meaningful to a wider audience.
Common Security Control	Security control that can be applied to one or more agency information systems and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

Term	Definition
	responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied.
Confidentiality	Assurance that information in an IT system is not disclosed to unauthorized persons, processes or devices.
Configuration Control	Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.
Configuration Management	The management of security features and assurances through the control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an automated information system (AIS).
Contingency Plan	A plan maintained for emergency response, backup operations, and post-disaster recovery for an IS, to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.
Countermeasures	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Defense in Depth	An approach for establishing an adequate computer security posture that integrates people, technology and operations. In the Defense in Depth approach, Security solutions are layered within and among IT assets to minimize single points of failure and security solutions are selected based on their relative level of robustness in view of the value of the asset protected. Implementation of this approach recognizes that the highly interactive nature of information systems and enclaves creates a shared risk environment; therefore, the adequate assurance of any single asset is dependent upon the adequate assurance of all interconnecting assets.
Executable Content	Executable content is a subset of mobile code that is largely invisible to the user and operates without a user decision. Executable content is automatically activated upon retrieval without user interaction.
Federal Enterprise Architecture (FEA)	A business-based framework for government-wide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based.
Firewall	A firewall system can be a router, a personal computer, a host, or a collection of hosts, set up specifically to shield a site or subnet from malicious hosts outside the site or subnet. A firewall system is usually located at a higher-level gateway, such as a site's connection to the Internet; however, firewall systems can be located at lower-level gateways to provide protection for some smaller collections of hosts or subnets. A firewall forces all network connections to pass through the gateway where they can be examined and evaluated, and provides other services such as advanced authentication measures to replace simple passwords. The firewall may then restrict access to or from selected systems, block certain Transmission Control Protocol/Internet Protocol (TCP/IP) services or provide other security features.
General Support System	An interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities and people, and provides support for a variety of

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

Term	Definition
	users and/or applications. Individual applications support different, mission-related functions. Users may be from the same or different organizations.
High-Impact System	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.
Host-based Security	The technique of securing an individual system from attack; host-based security is operating system and version dependent.
Identification and Authentication (I&A)	Identity of an entity with some level of assurance.
Impact	The cumulative effect upon an organization or its customers if a critical business process cannot be performed.
Information Resources	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information Technology	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. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Individual Accountability	Requires individual users to be held accountable for their actions after being notified of the rules of behavior in using the system and the penalties associated with the violation of those rules.
Integrity	Assurance that information in an IT system is protected from unauthorized, unanticipated, or unintentional modification or destruction. System integrity also addresses the quality of an IT system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data.
Intrusion Detection	Intrusion detection refers to the process of identifying attempts to penetrate a system and gain unauthorized access.
IT Security Policy Division (ITSMG)	The OCIO office responsible for the USPTO IT Security Program.
Key Management Infrastructure (KMI)	Framework established to issue, maintain, and revoke keys accommodating a variety of security technologies, including the use of software; the supporting infrastructure for a public key infrastructure (PKI).

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

Term	Definition
Least Privilege	Limiting permissions or privileges to those necessary to perform a specific job. This principle is implemented by assigning appropriate rights or privileges, as determined by the job performed and the permissions requested and approved by a supervisor, to each UserID/password combination. Also see Need to Know.
Low-Impact System	An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.
Major Application	<p>An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. Major applications include applications that meet the above definition, but at a minimum include applications that meet any one of the following criteria:</p> <ul style="list-style-type: none"> <li>Are mission critical;</li> <li>Are reviewed under agency's annual IT Investment review process</li> </ul>
Management Controls	Controls that address management of the security aspects of the IT system and the management of risk for the system. Management controls include risk management, review of security controls, system life cycle controls, processing authorization controls, and system security plan controls.
Material Weakness	A deficiency that the agency head determines to be significant enough to be reported outside the agency (i.e. included in the annual Integrity Act report to the President and the Congress) shall be considered a "material weakness." This designation requires a judgment by agency managers as to the relative risk and significance of deficiencies. Agencies may wish to use a different term to describe less significant deficiencies, which are reported only internally in an agency. In identifying and assessing the relative importance of deficiencies, particular attention should be paid to the views of the agency's IG.
Mobile Code	The term for code obtained from remote systems, transmitted across a network, and executed on a local system. Mobile code also refers to Web-based code downloaded and run by the user's browser. Mobile code refers to programs (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics. The term also applies to situations involving a large homogeneous collection of platforms (e.g., Microsoft Windows). Also see Active Content.
Moderate-Impact System	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high.
National Security Information	Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.
Need to Know	The concept of limiting access to information to those people who have a

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

<b>Term</b>	<b>Definition</b>
	need to see or use it in performing their jobs. Also see Least Privilege.
Non-repudiation	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
Operational Controls	Address security methods that focus on mechanisms primarily implemented and executed by people (as opposed to systems).
Operating System	An organized collection of techniques, procedures, programs, or routines for operating an information system.
Plan of Action and Milestones (POA&M)	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Potential Impact [FIPS 199]	The loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect (FIPS 199 low); (ii) a serious adverse effect (FIPS 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.
Privacy Impact Assessment	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.
Protection Needs Elicitation	The process of determining or eliciting from customers their information protection needs.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Residual Information	Data left in storage after processing operations are complete, but before degaussing or rewriting has taken place.
Residual Risk	The potential for the occurrence of an adverse event, after adjusting for the impact of all in-place safeguards. (See Acceptable Risk.)
Risk	The possibility of harm or loss to any software, information, hardware, administrative, physical, communications or personnel resource within an automated information system or activity. Risk is a measure of the likelihood and the consequence of events or acts that could cause a system compromise, including the unauthorized disclosure, destruction, removal, modification, or interruption of system assets.
Risk Analysis	An analysis of system assets and vulnerabilities to establish an expected loss from certain events, based on estimated probabilities of occurrence.
Risk Assessment	The process of identifying the risks to system security. This assessment includes determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis.
Risk Management	(1) The ongoing process of assessing the risk to automated information resources and information, as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate, cost-effective controls to achieve and maintain an acceptable level of risk. (2) The total process of

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

Term	Definition
	identifying, controlling, and mitigating information system-related risks. It includes risk assessment; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws.
Rules of Behavior	Established, implemented rules concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of Federal Government equipment, the assignment and limitation of system privileges, and individual accountability.
Safeguards	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Security Assurance	Security assurance is the degree of confidence that all security controls perform as intended to protect the system and the processed information.
Security Category [FIPS 199]	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.
Security Controls [FIPS 199]	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Impact Analysis	The analysis conducted by an agency official, often during the continuous monitoring phase of the security certification and accreditation process, to determine the extent to which changes to the information system have affected the security posture of the system.
Security Objective	Confidentiality, integrity, or availability.
Security Policy	What security means to the user; a statement of what is meant when claims of security are made. More formally, it is the set of rules and conditions governing the access and use of information. Typically, a security policy will refer to the conventional security services, such as confidentiality, integrity, availability, etc., and perhaps their underlying mechanisms and functions.
Security Violation	Any loss, misuse, unauthorized modification, disclosure of or access to information, applications, systems, networks and information technology infrastructure and resources.
Senior Agency Information Security Officer	
Sensitive Information	Refers to information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission; proprietary information; records about individuals requiring protection under the Privacy Act; and

**This document is uncontrolled when downloaded or printed. Before use, check the ITSMG intranet website to ensure you have the most current and official version.**

Term	Definition
	information not releasable under the Freedom of Information Act.
Signature (Digital, Electronic)	A process that operates on a message to assure message source authenticity and integrity, and may be required for source non-repudiation.
System Security Plan (SSP)	A document that identifies the information system components; operational environment; sensitivity and risks; and detailed, cost-effective measures to protect a system or group of systems. The SSP documents the system security requirements and how they are met throughout the life cycle of the system.
Target of Evaluation (TOE)	A Common Criteria term for an IT product or system and its associated administrator and user guidance documentation that is the subject of a security evaluation.
Technical Controls	Consist of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the IT system and applications. Sometimes called Technical Countermeasures.
Threat	An activity, deliberate or unintentional, with potential for causing harm to an automated information system or activity.
Token	A token is an object that represents something else, such as another object (either physical or virtual). A security token is a physical device, such as a special smart card, that together with something that a user knows, such as a PIN, will enable authorized access to a computer system or network.
User	Individual or (system) process authorized to access an information system.
Vulnerability	A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.
Workstation	Any computer connected to a Local Area Network (LAN). This includes personal computers, desktops, and information resources used or shared by one user.