

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
<b>MANAGEMENT CONTROLS</b>				
		<b>Risk Assessment</b>		
RA-1	A	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.		
RA-2	A	The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with FIPS 199 and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations		
RA-3	A	The organization conducts assessments 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.		
RA-4	A	The organization updates the risk assessment every three years or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.		
RA-5	MH	Vulnerability Scanning: Using appropriate vulnerability scanning tools and techniques, the organization scans for vulnerabilities in the information system every six months or when significant new vulnerabilities affecting the system are identified and reported.		
RA-5.1	H	Vulnerability scanning tools include the capability to readily update the list of vulnerabilities scanned.		

**LEGEND**

I = Implemented  
 NI = Not Implemented  
 P = Partially Implemented  
 NA = Not Applicable  
 AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
RA-5.2	H	Vulnerability Scanning: The organization updates the list of information system vulnerabilities every six months or when significant new vulnerabilities are identified and reported.		
RA-5.3	RB	Vulnerability scanning procedures include means to ensure adequate scan coverage, both vulnerabilities checked and information system components scanned.		
		<b>Planning</b>		
PL-1	A	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.		
PL-2	A	The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.		
PL-3	A	The organization reviews the security plan for the information system annually and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.		
PL-4	A	The organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system.		
PL-5	A	The organization conducts a privacy impact assessment on the information system.		
		<b>System and Services Acquisition</b>		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
SA-1	A	Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.		
SA-2	A	The organization determines, documents, and allocates as part of its capital planning and investment control process the resources required to adequately protect the information system.		
SA-3	A	The organization manages the information system using a system development life cycle methodology that includes information security considerations.		
SA-4	A	The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk.		
SA-5	A	The organization ensures that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel.		
SA-5.1	MH	The organization includes documentation describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.		
SA-5.2	H	The organization includes documentation describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).		
SA-6	A	The organization complies with software usage restrictions.		
SA-7	A	The organization enforces explicit rules governing the downloading and installation of software by users.		
SA-8	MH	The organization designs and implements the information system using security engineering principles.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
SA-9	A	The organization ensures that third-party providers of information system services employ adequate security controls in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements. The organization monitors security control compliance.		
SA-10	H	The information system developer creates and implements a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.		
SA-11	MH	The information system developer creates a security test and evaluation plan, implements the plan, and documents the results. Developmental security test results may be used in support of the security certification and accreditation process for the delivered information system.		
		<b>Certification, Accrediation, and Security Assessments</b>		
CA-1	A	The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.		
CA-2	MH	The organization conducts an assessment of the security controls in the information system annually 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.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
CA-3	A	The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary and monitors/controls the system interconnections on an ongoing basis. Appropriate organizational officials approve information system interconnection agreements.		
CA-4	A	The organization conducts an assessment of the security controls in the information system 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.		
CA-5	A	The organization develops and updates quarterly, a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.		
CA-6	A	The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization every 3 years. A senior organizational official signs and approves the security accreditation.		
CA-7	A	The organization monitors the security controls in the information system on an ongoing basis.		
<b>OPERATIONAL CONTROLS</b>				
		<b>Personnel Security</b>		
PS-1	A	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
PS-2	A	The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations periodically in accordance with OPM guidance.		
PS-3	A	The organization screens individuals requiring access to organizational information and information systems before authorizing access.		
PS-4	A	When employment is terminated, the organization terminates information system access, conducts exit interviews, ensures the return of all organizational information system-related property (e.g., keys, identification cards, building passes), and ensures that appropriate personnel have access to official records created by the terminated employee that are stored on organizational information systems.		
PS-5	A	The organization reviews information systems/facilities access authorizations when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorizations).		
PS-6	A	The organization completes appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for individuals requiring access to organizational information and information systems before authorizing access.		
PS-7	A	The organization establishes personnel security requirements for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management) and monitors provider compliance to ensure adequate security.		

**LEGEND**

I = Implemented  
 NI = Not Implemented  
 P = Partially Implemented  
 NA = Not Applicable  
 AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
PS-8	A	The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.		
		<b>Physical and Environmental Protection</b>		
PE-1	A	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, 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.		
PE-2	A	The organization develops and keeps current lists of personnel with authorized access to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and issues appropriate authorization credentials (e.g., badges, identification cards, smart cards). Designated officials within the organization review and approve the access list and authorization credentials once a year.		
PE-3	A	The organization controls all physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facilities. The organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.		
PE-4	RB	The organization controls physical access to information system transmission lines carrying unencrypted information to prevent eavesdropping, in-transit modification, disruption, or physical tampering.		

**LEGEND**

I = Implemented  
 NI = Not Implemented  
 P = Partially Implemented  
 NA = Not Applicable  
 AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
PE-5	MH	The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.		
PE-6	A	The organization monitors physical access to information systems to detect and respond to incidents. The organization monitors real-time intrusion alarms and surveillance equipment. The organization employs automated mechanisms to ensure potential intrusions are recognized and appropriate response actions initiated.		
PE-6.1	MH	The organization monitors real-time intrusion alarms and surveillance equipment.		
PE-6.2	H	The organization employs automated mechanisms to ensure potential intrusions are recognized and appropriate response actions initiated.		
PE-7	A	The organization controls physical access to information systems by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible.		
PE-7.1	MH	The organization escorts visitors and monitors visitor activity, when required.		
PE-8	A	The organization maintains a visitor access log to facilities (except for those areas within the facilities officially designated as publicly accessible) that includes: (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. Visitor logs are reviewed at closeout, maintained on file, and available for further review for one year.		
PE-8.1	MH	The organization employs automated mechanisms to facilitate the maintenance and review of access logs.		
PE-9	MH	The organization protects power equipment and power cabling for the information system from damage and destruction.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**



**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
PE-9.1	RB	The organization employs redundant and parallel power cabling paths.		
PE-10	MH	For specific locations within a facility containing concentrations of information system resources (e.g., data centers, server rooms, mainframe rooms), the organization provides the capability of shutting off power to any information technology component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the equipmen		
PE-11	MH	The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.		
PE-11.1	H	The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.		
PE-11.2	RB	The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.		
PE-12	A	The organization employs and maintains automatic emergency lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes.		
PE-13	A	The organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire..		
PE-13.1	MH	Fire suppression and detection devices/systems activate automatically in the event of a fire.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
PE-13.2	H	Fire suppression and detection devices/systems provide automatic notification of any activation to the organization and emergency responders.		
PE-14	A	The organization regularly maintains within acceptable levels and monitors the temperature and humidity within facilities containing information systems.		
PE-15	A	The organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel.		
PE-15.1	H	The organization employs automated mechanisms to automatically close shutoff valves in the event of a significant water leak.		
PE-16	A	The organization controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility and maintains appropriate records of those items.		
PE-17	MH	Individuals within the organization employ appropriate information system security controls at alternate work sites.		
<b>Contingency Planning</b>				
CP-1	A	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.		
CP-2	A	The organization develops and implements a contingency plan for the information system 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 organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.		

**LEGEND**

I = Implemented  
 NI = Not Implemented  
 P = Partially Implemented  
 NA = Not Applicable  
 AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
CP-2.1	MH	The organization coordinates contingency plan development with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).		
CP-3	MH	The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training annually.		
CP-3.1	H	The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.		
CP-3.2	RB	The organization employs automated mechanisms to provide a more thorough and realistic training		
CP-4	MH	The organization tests the contingency plan for the information system at least annually using to determine the plan's effectiveness and the organization's readiness to execute the plan. System rated as high shall be tested at the alternate processing site. Appropriate officials within the organization review the contingency plan test results and initiate corrective actions.		
CP-4.1	MH	The organization coordinates contingency plan testing with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).		
CP-4.2	H	The organization tests the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.		
CP-4.3	RB	The organization employs automated mechanisms to more thoroughly and effectively test the contingency		
CP-5	A	The organization reviews the contingency plan for the information system once per year and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
CP-6	MH	The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information. The alternate storage site is geographically separated from the primary storage site so as not to be susceptible to the same hazards.		
CP-6.1	MH	The alternate storage site is geographically separated from the primary storage site so as not to be susceptible to the same hazards.		
CP-6.2	H	The alternate storage site is configured to facilitate timely and effective recovery operations.		
CP-6.3	H	The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.		
CP-7	MH	The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within 24 hours when the primary processing capabilities are unavailable.		
CP-7.1	MH	The alternate processing site is geographically separated from the primary processing site so as not to be susceptible to the same hazards.		
CP-7.2	MH	The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.		
CP-7.3	MH	Alternate processing site agreements contain priority-of-service provisions in accordance with the organization's availability requirements.		
CP-7.4	H	The alternate processing site is fully configured to support a minimum required operational capability and ready to use as the operational site.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
CP-8	MH	The organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within 24 hours when the primary telecommunications capabilities are unavailable.		
CP-8.1	MH	Primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with the organization's availability requirements.		
CP-8.2	MH	Alternate telecommunications services do not share a single point of failure with primary telecommunications services.		
CP-8.3	H	Alternate telecommunications service providers are sufficiently separated from primary service providers so as not to be susceptible to the same hazards.		
CP-8.4	H	Primary and alternate telecommunications service providers have adequate contingency plans.		
CP-9	A	The organization conducts backups of user-level and system-level information (including system state information) contained in the information system according to backup schedules documented in the system contingency plan and stores backup information at an appropriately secured location.		
CP-9.1	MH	The organization conducts backups of user-level and system-level information (including system state information) contained in the information system according to backup schedules documented in the system contingency plan and stores backup information at an appropriately secured location.		
CP-9.2	H	The organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
CP-9.3	H	The organization stores backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.		
CP-10	A	The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to the system's original state after a disruption or failure.		
CP-10.1	H	The organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.		
		<b>Configuration Management</b>		
CM-1	A	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.		
CM-2	A	The organization develops, documents, and maintains a current, baseline configuration of the information system and an inventory of the system's constituent components.		
CM-2.1	MH	The organization updates the baseline configuration as an integral part of information system component installations. Plan includes explicit checks with assigned responsibilities to periodically ensure that the plan is being implemented as intended.		
CM-2.2	H	The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration.		
CM-3	MH	The organization documents and controls changes to the information system. Appropriate organizational officials approve information system changes in accordance with organizational policies and procedures.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
CM-3.1	H	The organization employs automated mechanisms to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.		
CM-4	MH	The organization monitors changes to the information system and conducts security impact analyses to determine the effects of the changes.		
CM-5	MH	The organization enforces access restrictions associated with changes to the information system.		
CM-5.1	H	The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.		
CM-6	A			
CM-6.1	H	The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.		
CM-7	MH	The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of any protocol or service that is not explicitly permitted.		
CM-7.1	H	The organization reviews the information system annually, to identify and eliminate unnecessary functions, ports, protocols, and/or services.		
		<b>Maintenance</b>		
MA-1	A	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
MA-2	A	The organization schedules, performs, and documents routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.		
MA-2.1	MH	The organization maintains a maintenance log for the information system that includes: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).		
MA-2.2	H	The organization employs automated mechanisms to ensure that periodic maintenance is scheduled and conducted as required, and that a log of maintenance actions, both needed and completed, is up to date, accurate, complete, and available.		
MA-3	MH	The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.		
MA-3.1	H	The organization inspects all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications.		
MA-3.2	H	The organization checks all media containing diagnostic test programs (e.g., software or firmware used for system maintenance or diagnostics) for malicious code before the media are used in the information system.		
MA-3.3	H	The organization checks all maintenance equipment with the capability of retaining information to ensure that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate organization official explicitly authorizes an exception.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**



**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
MA-3.4	RB	The organization employs automated mechanisms to ensure only authorized personnel use maintenance tools.		
MA-4	A	The organization approves, controls, and monitors remotely executed maintenance and diagnostic activities.		
MA-4.1	H	The organization audits all remote maintenance sessions, and appropriate organizational personnel review the audit logs of the remote sessions.		
MA-4.2	H	The organization addresses the installation and use of remote diagnostic links in the security plan for the information system.		
MA-4.3	H	Remote diagnostic or maintenance services are acceptable if performed by a service or organization that implements for its own information system the same level of security as that implemented on the information system being serviced.		
MA-5	A	The organization maintains a list of personnel authorized to perform maintenance on the information system. Only authorized personnel perform maintenance on the information system.		
MA-6	MH	The organization obtains maintenance support and spare parts within 48 hours of failure.		
		<b>System and Information Integrity</b>		
SI-1	A	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, 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.		
SI-2	A	The organization identifies, reports, and corrects information system flaws.		
SI-2.1	RB	The organization centrally manages the flaw remediation process and installs updates automatically without individual user intervention.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
SI-2.2	RB	The organization employs automated mechanisms to periodically and upon command determine the state of information system components with regard to flaw remediation.		
SI-3	A	The information system implements malicious code protection that includes a capability for automatic updates.		
SI-3.1	MH	The organization centrally manages virus protection mechanisms.		
SI-3.2	H	The information system automatically updates virus protection mechanisms.		
SI-4	MH	The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.		
SI-4.1	RB	The organization networks individual intrusion detection tools into a system-wide intrusion detection system using common protocols.		
SI-4.2	RB	The organization employs automated tools to support near-real-time analysis of events in support of detecting system-level attacks.		
SI-4.3	RB	The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.		
SI-4.4	RB	The information system monitors outbound communications for unusual or unauthorized activities indicating the presence of malware (e.g., malicious code, spyware, adware).		
SI-5	A	The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.		
SI-5.1	RB	The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
SI-6	MH	The information system verifies the correct operation of security functions periodically every year and notifies system administrator when anomalies are discovered.		
SI-6.1	H	The organization employs automated mechanisms to provide notification of failed security tests.		
SI-6.2	RB	The organization employs automated mechanisms to support management of distributed security testing.		
SI-7	H	The information system detects and protects against unauthorized changes to software and information.		
SI-8	MH	The information system implements spam and spyware protection.		
SI-8.1	H	The organization centrally manages spam and spyware protection mechanisms.		
SI-8.2	RB	The information system automatically updates spam and spyware protection mechanisms.		
SI-9	MH	The organization restricts the information input to the information system to authorized personnel only.		
SI-10	MH	The information system checks information inputs for accuracy, completeness, and validity.		
SI-11	MH	The information system identifies and handles error conditions in an expeditious manner.		
SI-12	MH	The organization handles and retains output from the information system in accordance with organizational policy and operational requirements.		
		<b>Media Protection</b>		
MP-1	A	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.		
MP-2	A	The organization ensures that only authorized users have access to information in printed form or on digital media removed from the information system.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
MP-2.1	H	Unless guard stations control access to media storage areas, the organization employs automated mechanisms to ensure only authorized access to such storage areas and to audit access attempts and access granted.		
MP-3	MH	The organization affixes external labels to removable information storage media and information system output indicating the distribution limitations and handling caveats of the information.		
MP-4	MH	The organization physically controls and securely stores information system media, both paper and electronic, based on the highest FIPS 199 security category of the information recorded on the media.		
MP-5	MH	The organization controls information system media (paper and electronic) and restricts the pickup, receipt, transfer, and delivery of such media to authorized personnel.		
MP-6	MH	The organization sanitizes information system digital media using approved equipment, techniques, and procedures. The organization tracks, documents, and verifies media sanitization actions and periodically tests sanitization equipment/procedures to ensure correct performance.		
MP-7	A	The organization sanitizes or destroys information system digital media before its disposal or release for reuse outside the organization, to prevent unauthorized individuals from gaining access to and using the information contained on the media.		
		<b>Incident Response</b>		
IR-1	A	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
IR-2	MH	The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training at least annually.		
IR-2.1	MH	The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.		
IR-2.2	H	The organization employs automated mechanisms to provide a more thorough and realistic training environment.		
IR-3	MH	The organization tests the incident response capability for the information system at least annually using automated mechanisms for high systems to determine the incident response effectiveness and documents the results.		
IR-3.1	H	The organization employs automated mechanisms to more thoroughly and effectively test the incident response capability.		
IR-4	A	The organization employs automated mechanisms to support the incident handling process.		
IR-4.1	MH	The organization employs automated mechanisms to support the incident handling process.		
IR-5	MH	The organization tracks and documents information system security incidents on an ongoing basis.		
IR-5.1	H	The organization tracks and documents information system security incidents on an ongoing basis.		
IR-6	A	The organization promptly reports incident information to appropriate authorities.		
IR-6	MH	The organization employs automated mechanisms to assist in the reporting of security incidents.		
IR-7	A	The organization provides an incident support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability.		
IR-7.1	MH	The organization employs automated mechanisms to increase the availability of incident response-related information and support.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
		<b>Awareness and Training</b>		
AT-1	A	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, 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.		
AT-2	A	The organization ensures all users (including managers and senior executives) are exposed to basic information system security awareness materials before authorizing access to the system and at least annually thereafter.		
AT-3	A	The organization identifies personnel with significant information system security roles and responsibilities, documents those roles and responsibilities, and provides appropriate information system security training before authorizing access to the system and each year thereafter.		
AT-4	A	The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.		
<b>TECHNICAL CONTROLS</b>				
		<b>Identification and Authentication</b>		
IA-1	A	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.		
IA-2	A	The information system uniquely identifies and authenticates users (or processes acting on behalf of users).		

**LEGEND**

I = Implemented  
 NI = Not Implemented  
 P = Partially Implemented  
 NA = Not Applicable  
 AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
IA-2.1	H	The information system employs multifactor authentication.		
IA-3	MH	The information system identifies and authenticates specific devices before establishing a connection.		
IA-4	A	The organization manages 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 organization official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier after 30 days of inactivity; and (vi) archiving user identifiers.		
IA-5	A	The organization manages information system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; and (iii) changing default authenticators upon information system installation.		
IA-6	A	The information system provides feedback to a user during an attempted authentication and that feedback does not compromise the authentication mechanism.		
IA-7	A	For authentication to a cryptographic module, the information system employs authentication methods that meet the requirements of FIPS 140-2.		
		<b>Access Control</b>		
AC-1	A	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
AC-2	A	The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts annually.		
AC-2.1	MH	The organization employs automated mechanisms to support the management of information system accounts.		
AC-2.2	MH	The information system automatically terminates temporary and emergency accounts after 48 hours.		
AC-2.3	MH	The information system automatically disables inactive accounts after 90 Days.		
AC-2.4	H	The organization employs automated mechanisms to ensure that account creation, modification, disabling, and termination actions are audited and, as required, appropriate individuals are notified.		
AC-3	A	The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.		
AC-3.1	MH	The information system ensures that access to security functions (deployed in hardware, software, and firmware) and information is restricted to authorized personnel (e.g., security administrators).		
AC-4	MH	The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.		
AC-5	MH	The information system enforces separation of duties through assigned access authorizations.		
AC-6	MH	The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**



**ORGANIZATION**  
**SYSTEM NAME**  
**MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
AC-7	A	The information system enforces a limit of three consecutive invalid access attempts by a user during a 30 minute time period. The information system automatically locks the account/node for 30 minutes for low systems or until an appropriate security administrator manually intervenes to unlocks accounts on moderate and high systems when the maximum number of unsuccessful attempts is exceeded.		
AC-7.1	RB	The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.		
AC-8	A	The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.		
AC-9	RB	The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.		
AC-10	H	The information system does not allow concurrent sessions for systems rated high.		
AC-11	MH	The information system prevents further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.		
AC-12	MH	The information system automatically terminates a session after ten minutes of inactivity.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
AC-13	A	The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.		
AC-13.1	H	The organization employs automated mechanisms to facilitate the review of user activities.		
AC-14	A	The organization identifies specific user actions that can be performed on the information system without identification or authentication.		
AC-14.1	MH	The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.		
AC-15	H	The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.		
AC-16	RB	The information system appropriately labels information in storage, in process, and in transmission.		
AC-17	A	The organization documents, monitors, and controls all methods of remote access (e.g., dial-up, Internet) to the information system including remote access for privileged functions. Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access method.		
AC-17.1	MH	The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.		
AC-17.2	MH	The organization uses encryption to protect the confidentiality of remote access sessions.		
AC-17.3	MH	The organization controls all remote accesses through a managed access control point.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
AC-18	MH	The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) documents, monitors, and controls wireless access to the information system. Appropriate organizational officials authorize the use of wireless technologies.		
AC-18.1	MH	The organization uses authentication and encryption to protect wireless access to the information system.		
AC-19	MH	The organization: (i) establishes usage restrictions and implementation guidance for portable and mobile devices; and (ii) documents, monitors, and controls device access to organizational networks. Appropriate organizational officials authorize the use of portable and mobile devices.		
AC-19.1	H	The organization employs removable hard drives or cryptography to protect information residing on portable and mobile devices.		
AC-20	A	The organization restricts the use of personally owned information systems for official U.S. Government business involving the processing, storage, or transmission of federal information.		
		<b>Audit and Accountability</b>		
AU-1	A	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.		
AU-2	A	The information system generates audit records for events identified in the HUD IT Security Handbook.		
AU-2.1	RB	The information system provides the capability to compile audit records from multiple components throughout the system into a system-wide (logical or physical), time-correlated audit trail.		

**LEGEND**

I = Implemented  
 NI = Not Implemented  
 P = Partially Implemented  
 NA = Not Applicable  
 AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
AU-2.2	RB	The information system provides the capability to manage the selection of events to be audited by individual components of the system.		
AU-3	A	The information system captures sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events.		
AU-3.1	MH	The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.		
AU-3.2	H	The information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.		
AU-4	A	The organization allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.		
AU-5	A	0		
AU-5.1	H	The information system provides a warning when allocated audit record storage volume is close to being reached.		
AU-6	MH	The organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.		
AU-6.1	H	The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.		
AU-6.2	RB	The organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications.		
AU-7	MH	The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
AU-7.1	H	The information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.		
AU-8	MH	The information system provides time stamps for use in audit record generation.		
AU-9	A	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.		
AU-9.1	RB	The information system produces audit information on hardware-enforced, write-once media.		
AU-10	RB	The information system provides the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message).		
AU-11	A	The organization retains audit logs in accordance with HUD records retention policies, but at least for one year for high and moderate systems to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.		
<b>Systems and Communications Protection</b>				
SC-1	A	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, 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.		
SC-2	MH	The information system separates user functionality (including user interface services) from information system management functionality.		
SC-3	H	The information system isolates security functions from nonsecurity functions.		
SC-3.1	H	The information system employs underlying hardware separation mechanisms to facilitate security function isolation.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION**  
**SYSTEM NAME**  
**MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
SC-3.2	H	: The information system further divides the security functions with the functions enforcing access and information flow control isolated and protected from both non-security functions and from other security functions.		
SC-3.3	H	The information system minimizes the amount of non-security functions included within the isolation boundary containing security functions.		
SC-3.4	H	The information system security maintains its security functions in largely independent modules that avoid unnecessary interactions between modules.		
SC-3.5	H	The information system security maintains its security functions in a layered structure minimizing interactions between layers of the design.		
SC-4	MH	The information system prevents unauthorized and unintended information transfer via shared system resources.		
SC-5	A	The information system protects against or limits the effects of denial of service attacks on devices within the organization's internal network.		
SC-5.1	RB	The information system restricts the ability of users to launch denial of service attacks against other information systems or networks.		
SC-5.2	RB	The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.		
SC-6	MH	The information system limits the use of resources by priority.		
SC-7	A	The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
SC-7.1	MH	The organization physically allocates publicly accessible information system components (e.g., public web servers) to separate subnetworks with separate, physical network interfaces. The organization prevents public access into the organization's internal networks except as appropriately mediated.		
SC-8	MH	The information system protects the integrity of transmitted information.		
SC-8.1	H	The organization employs cryptographic mechanisms to ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).		
SC-9	MH	The information system protects the confidentiality of transmitted information		
SC-9.1	H	The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless protected by alternative physical measures (e.g., protective distribution systems).		
SC-10	MH	The information system terminates a network connection at the end of a session or after ten minutes of inactivity.		
SC-11	RB	The information system establishes a trusted communications path between the user and the security functionality of the system.		
SC-12	MH	The information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management.		
SC-13	A	When cryptography is employed within the information system, the system performs all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation.		
SC-14	A	For publicly available systems, the information system protects the integrity of the information and applications.		

**LEGEND**

I = Implemented  
 NI = Not Implemented  
 P = Partially Implemented  
 NA = Not Applicable  
 AR = Accepting Risk

**OFFICIAL USE ONLY**

Page 31 of 32

**ORGANIZATION  
SYSTEM NAME  
MINIMUM SECURITY BASELINE ASSESSMENT**

9/18/2007

CONTORL	APPLICABILITY	SECURITY CONTROLS	STATUS	JUSTIFICATION/COMMENTS
SC-15	MH	The information system prohibits remote activation of collaborative computing mechanisms (e.g., video and audio conferencing) and provides an explicit indication of use to the local users (e.g., use of camera or microphone).		
SC-15.1	RB	The information system provides physical disconnect of camera and microphone in a manner that supports ease of use.		
SC-16	RB	The information system reliably associates security parameters (e.g., security labels and markings) with information exchanged between information systems.		
SC-17	MH	The organization develops and implements a certificate policy and certification practice statement for the issuance of public key certificates used in the information system.		
SC-18	MH	The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) documents, monitors, and controls the use of mobile code within the information system. Appropriate organizational officials authorize the use of mobile code.		
SC-19	MH	The organization: (i) establishes usage restrictions and implementation guidance for Voice Over Internet Protocol (VOIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) documents, monitors, and controls the use of VOIP within the information system. Appropriate organizational officials authorize the use of VOIP.		

**LEGEND**

I = Implemented  
NI = Not Implemented  
P = Partially Implemented  
NA = Not Applicable  
AR = Accepting Risk

**OFFICIAL USE ONLY**