Information Technology (IT) Contingency Planning (CP) Standard

November 17, 2023

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Questions about the policies outlined in this document should be directed to Information Assurance Services (IAS) at **OCIO_IAS@ed.gov**

APPROVAL

STEVEN HERNANDEZ

Digitally signed by STEVEN HERNANDEZ
Date: 2023.11.17 17:10:45 -05'00'

Steven Hernandez
Director, IAS/Chief Information Security Officer (CISO)

Revision History

The table below identifies all changes that have been incorporated into this document.

Version	Draft Date	Summary of Changes
1.0	1/14/2022	Initial draft of new standard which combines NIST SP 800-53, Revision 5 controls, including ED specific control parameter values, with existing policy standards.
1.1	1/31/2022	Update to incorporate feedback from IAS; address new security measures required by Executive Order (EO) 14028, including Office of Management and Budget (OMB) regulations and memoranda and updated National Institute of Standards and Technology (NIST) guidance issued to comply with the EO.
1.2	2/11/2022	Updates to CP-3 and CP-4
1.3	12/05/2022	Updates to Overlay CP-2 ED-02; addition of Overlay CP-4 ED-02.
5.4	11/17/2023	Aligned document major version number to align with NIST SP 800-53 revision number. Clean up formatting and numbering throughout and update broken links. Section 2, Standards was updated to include the description of incorporating organizationally defined parameters (ODP) for controls that may be necessary from external control overlays (e.g., High Value Assets [HVA]). Inserted references to NIST SP 800-53B tailoring guidance. Updated Section 4, Acronyms as appropriate. Updated language in controls CP-1, CP-02 ED-03, CP-04 ED-01, CP-04 ED-02, CP-7(1), CP-7(3), and CP-7(4). Added controls CP-2 ED-03 and CP-8(5). Added “leading zeros” to control identifiers in alignment with patch release of NIST Special Publication (SP) 800-53 (Release 5.1.1) to applicable controls, enhancements, and overlays.

Table of Contents

1 INTRODUCTION

This governance document establishes U.S. Department of Education (ED or Department) information technology (IT) contingency planning controls standards necessary to improve the efficiency of operation or security of Department information systems and comply with Federal laws, regulations, Executive Orders, Emergency Orders (EO), Binding Operational Directives (BOD), and Department Administrative Communications System Directives (ACSD) and Handbooks. In doing so, these standards supersede any prior governance documentation establishing such standards.

1.1 Purpose

The Federal Information Security Modernization Act (FISMA)[1] and implementing regulation Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*[2], requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, and services that are either fully or partially provided, including agency-hosted, outsourced, and cloud-based solutions. Federal Information Processing Standards (FIPS) Publication (PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems*[3], mandates the use of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*[4], as amended, as baseline information system controls.

1.2 Scope

These standards apply to all information and information systems that support the operations and assets of the Department, including those provided or managed by another agency, contractor, or other source, as well as services that are either fully or partially provided, including Department-hosted, outsourced, and cloud-based solutions. Principal Offices, employees, contractors, external service providers and system users are required to comply with these contingency planning control standards.

[1] Public Law 113-283-Dec. 18, 2014, https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[2] Office of Management and Budget (OMB) Circular A-130, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf
[3] FIPS 200, https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.200.pdf
[4] NIST SP 800-53, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

2 STANDARDS

The Department standards for IT Contingency Planning controls are organized to follow the order in which controls are presented in the current version of NIST SP 800-53. To define a control baseline for Department information systems, a FIPS PUB 199 categorization level (e.g., Low [L], Moderate [M] and High [H]) is assigned to each requirement. This designator indicates a requirement applies to information systems categorized at that FIPS PUB 199 impact-level. Designators are also used to indicate when NIST SP 800-53 Privacy baseline controls (e.g., Privacy (P) are required. To manage risk to within the Department's risk tolerance and appetite, control overlays are provided when the Department requires implementation of control(s) that are not required by the FIPS PUB 199 impact-level or privacy baseline.

In addition to the controls required by this standard, High Value Assets (HVAs) must implement and comply with the current version of the HVA Control Overlays[5] issued and maintained by the U.S. Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA). Systems that process federal tax return information (FTRI) must implement and comply with the Internal Revenue Service (IRS) Publication 1075[6], *Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information.* Systems that are Federal Risk and Authorization Management Program (FedRAMP) authorized must implement and comply with the FedRAMP identified baselines[7].

Throughout the standard, there are controls captured that have not been scoped to any specific security or privacy baseline. This is intentional as all controls for identified external overlays and baselines (e.g., FedRAMP, IRS, HVA), that may apply to systems within the Department, have been incorporated into the standard. This ensures the organization defined parameters (ODPs) for controls within the Department have been clearly defined in a consistent manner.

Based upon an assessment of risk and determination that the level of protection for the security-relevant information within a system is not adversely impacted, contingency planning controls identified in the current version of NIST SP 800-53B that support only the availability security objective may be downgraded to the corresponding contingency planning control in a lower baseline (or modified or eliminated if not defined in a lower baseline).

This standard directly supports the Department's integration of the NIST Cybersecurity Framework (CSF) and NIST Privacy Framework (PF) by using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the Department's risk management processes. Refer to ***APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY*** for a summary of controls by baseline and corresponding NIST CSF and NIST PF categories and subcategories.

[5] HVA Control Overlay https://www.cisa.gov/publication/high-value-asset-control-overlay
[6] IRS Publication 1075 https://www.irs.gov/pub/irs-pdf/p1075.pdf
[7] FedRAMP baselines https://www.fedramp.gov/baselines/

2.1 CP-01 Policy and Procedures (L, M, H)

The Department shall develop, document, and disseminate to all ED employees, contractors, and users authorized to access to ED information systems, or systems operated or maintained on behalf of ED, or ED information as defined in ACSD-OCIO-004[8], *Cybersecurity Policy* a Department-level IT Contingency Planning policy (e.g., this document) that:

(a) addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

(c) authorizes the Department Chief Information Security Officer (CISO) and Department Chief Information Officer (CIO) to issue subordinate standards, procedures, and memos, with the same authority and enforcement as ACSD-OCIO-004, Cybersecurity Policy.

The Department CISO in conjunction with the Senior Agency Official for Privacy (SAOP) are designated to manage the development, documentation, and dissemination of the Department-level IT system contingency planning policy.

This policy shall be reviewed and updated annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

Principal Office Information System Owners (ISO) and Information System Security Officers (ISSOs) are required to manage the development, documentation, and dissemination of system specific procedures to facilitate the implementation of the Department's IT system contingency planning policy and the associated controls. The ISO and ISSO shall review IT system contingency planning procedures annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

2.2 CP-02 Contingency Plan (L, M, H and Control Overlay)

a. Develop a contingency plan for the system that:

   1. Identifies essential mission and business functions and associated contingency requirements;

[8] Also known as OCIO: 3-112

2. Provides recovery objectives, restoration priorities, and metrics;
3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;
5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;
6. Addresses the sharing of contingency information; and
7. Is reviewed and approved by the ISO and the ISSO;

b. Distribute copies of the contingency plan to key contingency personnel, to include all response team personnel such as Telecommunications team;

c. Coordinate contingency planning activities with incident handling activities;

d. Review the contingency plan for the system annually;

e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Communicate contingency plan changes to ISSO, ISO, and other key contingency personnel;

g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and

h. Protect the contingency plan from unauthorized disclosure and modification.

Control Overlay CP-02, ED-01 (L, M, H): Use the current version of the Department approved Information System Contingency Plan (ISCP) template and Business Impact Analysis (BIA) template to develop and maintain the plan required by this control; use of these templates is not required for cloud service providers and Shared Services.

Control Overlay CP-02, ED-02 (M, H): Use the current version of the Department approved Disaster Recovery Plan (DRP) template to develop and maintain a DRP; development of a DRP is not required for subsystems, cloud service providers and Shared Services.

Control Overlay CP-02, ED-03 (L, M, H): Use the output of the BIA to support Enterprise Risk Management (ERM) and Cybersecurity Risk Management (CSRM) processes, as described in the NIST Interagency Report (IR) 8286 series, and to enable consistent prioritization, response, and communication regarding information security risk.

2.2.1 CP-02(01) Contingency Plan | Coordinate with Related Plans (M, H)[9]

Coordinate contingency plan development with organizational elements responsible for related plans.

2.2.2 CP-02(02) Contingency Plan | Capacity Planning (H)[9]

Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

2.2.3 CP-02(03) Contingency Plan | Resume Mission and Business Functions (M, H)[9]

Plan for the resumption of mission essential functions (MEF), national essential functions (NEF), and mission and business functions within system-level specified timeframes and metrics defined in the ISCP and BIA of contingency plan activation.

2.2.4 CP-02(05) Contingency Plan | Continue Mission and Business Functions (H)[9]

Plan for the continuance of MEF and NEF, as documented within the Department Continuity of Operations Plan (COOP), mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.

2.2.5 CP-02(08) Contingency Plan | Identify Critical Assets (M, H and Control Overlay)[9]

Identify critical system assets supporting critical and essential mission and business functions, as documented within the Department COOP.

Control Overlay CP-02(08), ED-01 (M, H): Document all mission critical systems within the Cyber Security Assessment and Management (CSAM) tool and Department COOP.

Control Overlay CP-02(08), ED-02 (M, H): Identify systems which support one or more MEF/NEF, document these systems within CSAM, and ensure System Security Plans contain adequate documentation for traceability to the Department COOP.

2.3 CP-03 Contingency Training (L, M, H)

a. Provide contingency training to system users consistent with assigned roles and responsibilities:

   1. Within thirty (30) days of assuming a contingency role or responsibility;
   2. When required by system changes; and
   3. Annually (i.e., each fiscal year) thereafter; and

[9] CP-2(1), CP-2(2), CP-2(3), CP-2(5), and CP-2(8) have been identified by NIST SP 800-53B as supporting only availability and may be downgraded to the corresponding control in a lower baseline (or modified or eliminated if defined in a lower baseline) only if the downgrading action reflects the security category for the supported availability security objective defined impact level.

b. Review and update contingency training content annually (i.e., each fiscal year) and following events to include but not limited to contingency plan test, lessons learned, assessment or audit findings, security incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Note: not required for cloud service providers or Shared Services.

2.3.1 CP-03(01) Contingency Training | Simulated Events (H)[10]

Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.

2.4 CP-04 Contingency Plan Testing (L, M, H and Control Overlay)

a. Test the contingency plan for the system at least annually and following major system changes using the following tests to determine the effectiveness of the plan and the readiness to execute the plan:

   1. Low-impact system: conduct annual tabletop exercise;
   2. Moderate-impact system: conduct annual tabletop or functional exercise; and
   3. High-impact systems conduct full-scale functional exercise to include system failover to the alternate location.

b. Review the contingency plan test results; and

c. Initiate corrective actions, if needed.

Control Overlay CP-04 ED-01 (L, M, H): Cloud Service Providers (CSPs) and Shared Services are not required to upload contingency plan test (CPT) artifacts in CSAM. However, testing dates must be entered into CSAM for all systems.

Control Overlay CP-04 ED-02 (M, H): Test the disaster recovery plan for the system annually and following major system changes to determine the effectiveness of the plan and the readiness to execute the plan. For new systems, ensure system is stable in production for a period of no less than six months before performing DRP testing with DRP testing completed no later than one year from the initial ATO. Upload disaster recovery plan test (DRPT) artifacts into CSAM. DRP testing is not required for subsystems, cloud service providers and Shared Services.

2.4.1 CP-04(01) Contingency Plan Testing | Coordinate with Related Plans (M, H)[10]

Coordinate contingency plan testing with organizational elements responsible for related plans.

[10] CP-3(1), and CP-4(1) have been identified by NIST SP 800-53B as supporting only availability and may be downgraded to the corresponding control in a lower baseline (or modified or eliminated if defined in a lower baseline) only if the downgrading action reflects the security category for the supported availability security objective defined impact level.

2.4.2 CP-04(02) Contingency Plan Testing | Alternate Processing Site (H)[11]

Test the contingency plan at the alternate processing site:

a. To familiarize contingency personnel with the facility and available resources; and

b. To evaluate the capabilities of the alternate processing site to support contingency operations.

2.5 CP-06 Alternate Storage Site (M, H)[11]

a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and

b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

2.5.1 CP-06(01) Alternate Storage Site | Separation from Primary Site (M, H)[11]

Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.

2.5.2 CP-06(02) Alternate Storage Site | Recovery Time and Recovery Point Objectives (H)[11]

Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

2.5.3 CP-06(03) Alternate Storage Site | Accessibility (M, H)[11]

Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

2.6 CP-07 Alternate Processing Site (M, H)[11]

a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of information system operations for essential mission and business functions within the time period defined in the system ISCP when the primary processing capabilities are unavailable;

b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and

[11] CP-4(2), CP-6, CP-6(1), CP-6(2), CP-6(3), and CP-7 have been identified by NIST SP 800-53B as supporting only availability and may be downgraded to the corresponding control in a lower baseline (or modified or eliminated if defined in a lower baseline) only if the downgrading action reflects the security category for the supported availability security objective defined impact level.

c. Provide controls at the alternate processing site that are equivalent to those at the primary site.

2.6.1 CP-07(01) Alternate Processing Site | Separation from Primary Site (M, H)[12]

Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

2.6.2 CP-07(02) Alternate Processing Site | Accessibility (M, H)[12]

Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

2.6.3 CP-07(03) Alternate Processing Site | Priority of Service (M, H)[12]

Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).

2.6.4 CP-07(04) Alternate Processing Site | Preparation for Use (H)[12]

Prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions.

2.7 CP-08 Telecommunications Services (M, H)[12]

Establish alternate telecommunications services, including necessary agreements to permit the resumption of information system operations for essential mission and business functions within the specified timeframes and metrics defined in the ISCP and BIA when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

2.7.1 CP-08(01) Telecommunications Services | Priority of Service Provisions (M, H)[12]

a. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and

b. Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

2.7.2 CP-08(02) Telecommunications Services | Single Points of Failure (M, H)[12]

Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

[12] CP-7(1), CP-7(2), CP-7(3), CP-7(4), CP-8, CP-8(1), and CP-8(2) have been identified by NIST SP 800-53B as supporting only availability and may be downgraded to the corresponding control in a lower baseline (or modified or eliminated if defined in a lower baseline) only if the downgrading action reflects the security category for the supported availability security objective defined impact level.

2.7.3 CP-08(03) Telecommunications Services | Separation of Primary and Alternate Providers (H)[13]

Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

2.7.4 CP-08(04) Telecommunications Services | Provider Contingency Plan (H)[13]

a. Require primary and alternate telecommunications service providers to have contingency plans;

b. Review provider contingency plans to ensure that the plans meet organizational contingency requirements; and

c. Obtain evidence of contingency testing and training by providers as needed but no less than annually.

2.7.5 CP-08(05) Telecommunications Services | Alternate Telecommunication Service Testing[13]

Test alternate telecommunication services at least every 6 months.

2.8 CP-09 System Backup (L, M, H and Control Overlay)

a. Conduct backups of user-level information contained in all system components in the authorization boundary with incremental daily backups and monthly full backups or at a frequency consistent with the recovery time and recovery point objectives.

b. Conduct backups of system-level information contained all system components in the authorization boundary with incremental daily backups and monthly full backups or at a frequency consistent with the recovery time and recovery point objectives.

c. Conduct backups of system documentation, including security- and privacy-related documentation with incremental daily backups and monthly full backups or at a frequency consistent with the recovery time and recovery point objectives.

d. Protect the confidentiality, integrity, and availability of backup information.

Control Overlay CP-09, ED-01 (M, H): Back up data, exercise backup restoration, and be prepared to recover data used by EO-critical software and EO-critical software platforms at any time from backups.

[13] CP-8(3), CP-8(4), and CP-8(5) have been identified by NIST SP 800-53B as supporting only availability and may be downgraded to the corresponding control in a lower baseline (or modified or eliminated if defined in a lower baseline) only if the downgrading action reflects the security category for the supported availability security objective defined impact level.

2.8.1 CP-09(01) System Backup | Testing for Reliability and Integrity (M, H)

Test backup information at least annually (i.e., each fiscal year) to verify media reliability and information integrity.

2.8.2 CP-09(02) System Backup | Test Restoration Using Sampling (H)[14]

Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.

2.8.3 CP-09(03) System Backup | Separate Storage for Critical Information (H)[14]

Store backup copies of current response plans and all supporting documentation, critical system software (including operating systems, cryptographic key management systems, and intrusion detection/prevention systems), as well as copies of the system inventory (including hardware, software, and firmware components) in a separate facility or in a fire rated container that is not collocated with the operational system.

2.8.4 CP-09(05) System Backup | Transfer to Alternate Storage Site (H)[14]

Transfer system backup information to the alternate storage site at a transfer rate consistent with the specified timeframes and metrics defined in the ISCP and BIA.

2.8.5 CP-09(08) System Backup | Cryptographic Protection (M, H)

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of all system backup information in storage at both primary and alternate locations when an alternate location is required and in place.

2.9 CP-10 System Recovery and Reconstitution (L, M, H)

Provide for the recovery and reconstitution of the system to a known state within system-level specified recovery times and metrics defined in the ISCP and BIA after a disruption, compromise, or failure.

2.9.1 CP-10(02) System Recovery and Reconstitution | Transaction Recovery (M, H)[14]

Implement transaction recovery for systems that are transaction-based.

2.9.2 CP-10(04) System Recovery and Reconstitution | Restore Within Time Period (H)[14]

Provide the capability to restore system components within system-level specified recovery times and metrics defined in the ISCP and BIA from configuration-controlled and integrity-protected information representing a known, operational state for the components.

[14] CP-9(2), CP-9(3), CP-9(5), CP-10(2), and CP-10(4) have been identified by NIST SP 800-53B as supporting only availability and may be downgraded to the corresponding control in a lower baseline (or modified or eliminated if defined in a lower baseline) only if the downgrading action reflects the security category for the supported availability security objective defined impact level.

3 RISK ACCEPTANCE/POLICY EXCEPTIONS

Deviations from the Department policies, Instructions, Standards, Procedures or Memos must be approved and documented through the Department's Risk Acceptance process. Deviations that introduce additional risks to the enterprise must be submitted through the Department Risk Acceptance Form (RAF) and must be approved by the ED CISO (as delegated). Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information, if applicable. Policy deviations that do not introduce additional risks do not need to be submitted through the Department RAF but will need to be approved by the Department CISO (as delegated).

4 ACRONYMS

Acronym	Definition
ACSD	Administrative Communications System Directives
BIA	Business Impact Analysis
BOD	Binding Operational Directives
CISA	Cybersecurity & Infrastructure Security Agency
CISO	Chief Information Security Officer
COOP	Continuity of Operations
CP	Contingency Planning Family
CPT	Contingency Plan Test
CSAM	Cyber Security Assessment and Management
CSF	Cybersecurity Framework
CSP	Cloud Service Provider
CSRM	Cybersecurity Risk Management
DE	Detect
DE.AE	Anomalies and Events
DE.DP	Detection Processes
Department	U.S. Department of Education
DHS	U.S. Department of Homeland Security
DRP	Disaster Recovery Plan
DRPT	Disaster Recovery Plan Test
ED	U.S. Department of Education
EO	Executive Order
ERM	Enterprise Risk Management
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FTRI	Federal Tax Return Information
GV.AT-P	Awareness and Training
GV.MT-P	Monitoring and Review
GV.PO-P	Governance Policies, Processes, and Procedures
GV-P	Govern-P
H	High
HVA	High Value Assets
IAS	Information Assurance Services
ICSP	Information System Contingency Plan
ID	Identify
ID.AM	Asset Management
ID.BE	Business Environment
ID.RA	Risk Assessment
ID.SC	Supply Chain Risk Management
IR	Interagency Report
IRS	Internal Revenue Service
ISO	Information System Owner
ISSO	Information System Security Officer

Acronym	Definition
IT	Information Technology
L	Low
M	Moderate
MEF	Mission Essential Function
NEF	National Essential Function
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
ODP	Organizationally Defined Parameters
OMB	Office of Management and Budget
P	Privacy
PF	Privacy Framework
PR	Protect
PR.AT	Awareness and Training
PR.DS	Data Security
PR.DS-P	Data Security
PR.IP	Information Protection Processes and Procedures
PR.PO-P	Data Protection Policies, Processes, and Procedures
PR.PT	Protective Technology
PR.PT-P	Protective Technology
PR-P	Protect-P
PUB	Publication
RAF	Risk Acceptance Form
RC	Recover
RC.CO	Communications
RC.IM	Improvements
RC.RP	Recovery Planning
RS	Respond
RS.AN	Analysis
RS.CO	Communications
RS.IM	Improvements
RS.RP	Response Planning
SAOP	Senor Agency Official for Privacy
SP	Special Publication

APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY

The applicability for each baseline control parameter is shown below.

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
CP-01	Policy and Procedures		X	X	X	PR.IP, DE.DP, GV.PO-P, GV.MT-P, PR.PO-P	PR.IP-9, DE.DP-2, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, PR.PO-P7
CP-02	Contingency Plan		X	X	X	ID.AM, ID.BE, ID.RA, ID.SC, PR.DS, PR.IP, DE.AE, RS.RP, RS.CO, RS.AN, RS.IM, RC.IM, RC.CO, GV.PO-P, PR.PO-P, PR.DS-P	ID.AM-5, ID.AM-6, ID.BE-4, ID.BE-5, ID.RA-4, ID.SC-5, PR.DS-4, PR.IP-7, PR.IP-8, PR.IP-9, DE.AE-3, DE.AE-4, RS.RP-1, RS.CO-1, RS.CO-3, RS.CO-4, RS.AN-2, RS.AN-4, RS.IM-1, RS.IM-2, RC.IM-1, RC.IM-2, RC.CO-3, GV.PO-P3, PR.PO-P5, PR.PO-P6, PR.PO-P7, PR.DS-P4
CP-02(01)	Contingency Plan | Coordinate with Related Plans			X	X	ID.AM, ID.BE, ID.RA, ID.SC, PR.DS, PR.IP, DE.AE, RS.RP,	ID.AM-5, ID.AM-6, ID.BE-4, ID.BE-5, ID.RA-4, ID.SC-5, PR.DS-4, PR.IP-7,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
						RS.CO, RS.AN, RS.IM, RC.IM, RC.CO, GV.PO-P, PR.PO-P, PR.DS-P	PR.IP-8, PR.IP-9, DE.AE-3, DE.AE-4, RS.RP-1, RS.CO-1, RS.CO-3, RS.CO-4, RS.AN-2, RS.AN-4, RS.IM-1, RS.IM-2, RC.IM-1, RC.IM-2, RC.CO-3, GV.PO-P3, PR.PO-P5, PR.PO-P6, PR.PO-P7, PR.DS-P4
CP-02(02)	Contingency Plan | Capacity Planning				X	ID.AM, ID.BE, ID.RA, ID.SC, PR.DS, PR.IP, DE.AE, RS.RP, RS.CO, RS.AN, RS.IM, RC.IM, RC.CO, GV.PO-P, PR.PO-P, PR.DS-P	ID.AM-5, ID.AM-6, ID.BE-4, ID.BE-5, ID.RA-4, ID.SC-5, PR.DS-4, PR.IP-7, PR.IP-8, PR.IP-9, DE.AE-3, DE.AE-4, RS.RP-1, RS.CO-1, RS.CO-3, RS.CO-4, RS.AN-2, RS.AN-4, RS.IM-1, RS.IM-2, RC.IM-1, RC.IM-2, RC.CO-3, GV.PO-P3, PR.PO-P5, PR.PO-P6, PR.PO-P7, PR.DS-P4
CP-02(03)	Contingency Plan | Resume Mission and Business Functions			X	X	ID.AM, ID.BE, ID.RA, ID.SC,	ID.AM-5, ID.AM-6, ID.BE-4, ID.BE-5,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
						PR.DS, PR.IP, DE.AE, RS.RP, RS.CO, RS.AN, RS.IM, RC.IM, RC.CO, GV.PO-P, PR.PO-P, PR.DS-P	ID.RA-4, ID.SC-5, PR.DS-4, PR.IP-7, PR.IP-8, PR.IP-9, DE.AE-3, DE.AE-4, RS.RP-1, RS.CO-1, RS.CO-3, RS.CO-4, RS.AN-2, RS.AN-4, RS.IM-1, RS.IM-2, RC.IM-1, RC.IM-2, RC.CO-3, GV.PO-P3, PR.PO-P5, PR.PO-P6, PR.PO-P7, PR.DS-P4
CP-02(05)	Contingency Plan | Continue Mission and Business Functions				X	ID.AM, ID.BE, ID.RA, ID.SC, PR.DS, PR.IP, DE.AE, RS.RP, RS.CO, RS.AN, RS.IM, RC.IM, RC.CO, GV.PO-P, PR.PO-P, PR.DS-P	ID.AM-5, ID.AM-6, ID.BE-4, ID.BE-5, ID.RA-4, ID.SC-5, PR.DS-4, PR.IP-7, PR.IP-8, PR.IP-9, DE.AE-3, DE.AE-4, RS.RP-1, RS.CO-1, RS.CO-3, RS.CO-4, RS.AN-2, RS.AN-4, RS.IM-1, RS.IM-2, RC.IM-1, RC.IM-2, RC.CO-3, GV.PO-P3, PR.PO-P5, PR.PO-P6, PR.PO-P7, PR.DS-P4

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
CP-02(06)	Contingency Plan | Alternate Processing and Storage Sites					ID.AM, ID.BE, ID.RA, ID.SC, PR.DS, PR.IP, DE.AE, RS.RP, RS.CO, RS.AN, RS.IM, RC.IM, RC.CO, GV.PO-P, PR.PO-P, PR.DS-P	ID.AM-5, ID.AM-6, ID.BE-4, ID.BE-5, ID.RA-4, ID.SC-5, PR.DS-4, PR.IP-7, PR.IP-8, PR.IP-9, DE.AE-3, DE.AE-4, RS.RP-1, RS.CO-1, RS.CO-3, RS.CO-4, RS.AN-2, RS.AN-4, RS.IM-1, RS.IM-2, RC.IM-1, RC.IM-2, RC.CO-3, GV.PO-P3, PR.PO-P5, PR.PO-P6, PR.PO-P7, PR.DS-P4
CP-02(07)	Contingency Plan | Coordinate with External Service Providers					ID.AM, ID.BE, ID.RA, ID.SC, PR.DS, PR.IP, DE.AE, RS.RP, RS.CO, RS.AN, RS.IM, RC.IM, RC.CO, GV.PO-P, PR.PO-P, PR.DS-P	ID.AM-5, ID.AM-6, ID.BE-4, ID.BE-5, ID.RA-4, ID.SC-5, PR.DS-4, PR.IP-7, PR.IP-8, PR.IP-9, DE.AE-3, DE.AE-4, RS.RP-1, RS.CO-1, RS.CO-3, RS.CO-4, RS.AN-2, RS.AN-4, RS.IM-1, RS.IM-2, RC.IM-1, RC.IM-2, RC.CO-3, GV.PO-P3,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
							PR.PO-P5, PR.PO-P6, PR.PO-P7, PR.DS-P4
CP-02(08)	Contingency Plan | Identify Critical Assets			X	X	ID.AM, ID.BE, ID.RA, ID.SC, PR.DS, PR.IP, DE.AE, RS.RP, RS.CO, RS.AN, RS.IM, RC.IM, RC.CO, GV.PO-P, PR.PO-P, PR.DS-P	ID.AM-5, ID.AM-6, ID.BE-4, ID.BE-5, ID.RA-4, ID.SC-5, PR.DS-4, PR.IP-7, PR.IP-8, PR.IP-9, DE.AE-3, DE.AE-4, RS.RP-1, RS.CO-1, RS.CO-3, RS.CO-4, RS.AN-2, RS.AN-4, RS.IM-1, RS.IM-2, RC.IM-1, RC.IM-2, RC.CO-3, GV.PO-P3, PR.PO-P5, PR.PO-P6, PR.PO-P7, PR.DS-P4
CP-03	Contingency Training		X	X	X	PR.AT, RS.CO, GV.AT-P	PR.AT-5, RS.CO-1, GV.AT-P3
CP-03(01)	Contingency Training | Simulated Events				X	PR.AT, RS.CO, GV.AT-P	PR.AT-5, RS.CO-1, GV.AT-P3
CP-03(02)	Contingency Training | Mechanisms Used in Training Environments					PR.AT, RS.CO, GV.AT-P	PR.AT-5, RS.CO-1, GV.AT-P3
CP-04	Contingency Plan Testing		X	X	X	ID.SC, PR.IP, PR.PO-P	ID.SC-5, PR.IP-4, PR.IP-7, PR.IP-10, PR.PO-P3, PR.PO-P5, PR.PO-P8
CP-04(01)	Contingency Plan Testing | Coordinate with Related Plans			X	X	ID.SC, PR.IP, PR.PO-P	ID.SC-5, PR.IP-4, PR.IP-7,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
							PR.IP-10, PR.PO-P3, PR.PO-P5, PR.PO-P8
CP-04(02)	Contingency Plan Testing | Alternate Processing Site				X	ID.SC, PR.IP, PR.PO-P	ID.SC-5, PR.IP-4, PR.IP-7, PR.IP-10, PR.PO-P3, PR.PO-P5, PR.PO-P8
CP-04(03)	Contingency Plan Testing | Automated Testing					ID.SC, PR.IP, PR.PO-P	ID.SC-5, PR.IP-4, PR.IP-7, PR.IP-10, PR.PO-P3, PR.PO-P5, PR.PO-P8
CP-04(04)	Contingency Plan Testing | Full Recovery and Reconstitution					ID.SC, PR.IP, PR.PO-P	ID.SC-5, PR.IP-4, PR.IP-7, PR.IP-10, PR.PO-P3, PR.PO-P5, PR.PO-P8
CP-04(05)	Contingency Plan Testing | Self-challenge					ID.SC, PR.IP, PR.PO-P	ID.SC-5, PR.IP-4, PR.IP-7, PR.IP-10, PR.PO-P3, PR.PO-P5, PR.PO-P8
CP-06	Alternate Storage Site			X	X	PR.IP, PR.PO-P	PR.IP-4, PR.PO-P3
CP-06(01)	Alternate Storage Site | Separation from Primary Site			X	X	PR.IP, PR.PO-P	PR.IP-4, PR.PO-P3
CP-06(02)	Alternate Storage Site | Recovery Time and Recovery Point Objectives				X	PR.IP, PR.PO-P	PR.IP-4, PR.PO-P3
CP-06(03)	Alternate Storage Site | Accessibility			X	X	PR.IP, PR.PO-P	PR.IP-4, PR.PO-P3
CP-07	Alternate Processing Site			X	X	PR.IP, PR.PT, PR.PO-P, PR.PT-P	PR.IP-9, PR.PT-5, PR.PO-P7, PR.PT-P4
CP-07(01)	Alternate Processing Site | Separation from Primary Site			X	X	PR.IP, PR.PT, PR.PO-P, PR.PT-P	PR.IP-9, PR.PT-5, PR.PO-P7, PR.PT-P4

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
CP-07(02)	Alternate Processing Site | Accessibility			X	X	PR.IP, PR.PT, PR.PO-P, PR.PT-P	PR.IP-9, PR.PT-5, PR.PO-P7, PR.PT-P4
CP-07(03)	Alternate Processing Site | Priority of Service			X	X	PR.IP, PR.PT, PR.PO-P, PR.PT-P	PR.IP-9, PR.PT-5, PR.PO-P7, PR.PT-P4
CP-07(04)	Alternate Processing Site | Preparation for Use				X	PR.IP, PR.PT, PR.PO-P, PR.PT-P	PR.IP-9, PR.PT-5, PR.PO-P7, PR.PT-P4
CP-07(06)	Alternate Processing Site | Inability to Return to Primary Site					PR.IP, PR.PT, PR.PO-P, PR.PT-P	PR.IP-9, PR.PT-5, PR.PO-P7, PR.PT-P4
CP-08	Telecommunications Services			X	X	ID.BE, PR.PT, PR.PT-P	ID.BE-4, PR.PT-4, PR.PT-5, PR.PT-P3, PR.PT-P4
CP-08(01)	Telecommunications Services | Priority of Service Provisions			X	X	ID.BE, PR.PT, PR.PT-P	ID.BE-4, PR.PT-4, PR.PT-5, PR.PT-P3, PR.PT-P4
CP-08(02)	Telecommunications Services | Single Points of Failure			X	X	ID.BE, PR.PT, PR.PT-P	ID.BE-4, PR.PT-4, PR.PT-5, PR.PT-P3, PR.PT-P4
CP-08(03)	Telecommunications Services | Separation of Primary and Alternate Providers				X	ID.BE, PR.PT, PR.PT-P	ID.BE-4, PR.PT-4, PR.PT-5, PR.PT-P3, PR.PT-P4
CP-08(04)	Telecommunications Services | Provider Contingency Plan				X	ID.BE, PR.PT, PR.PT-P	ID.BE-4, PR.PT-4, PR.PT-5, PR.PT-P3, PR.PT-P4
CP-08(05)	Telecommunications Services | Alternate Telecommunication Service Testing					ID.BE, PR.PT, PR.PT-P	ID.BE-4, PR.PT-4, PR.PT-5, PR.PT-P3, PR.PT-P4
CP-09	System Backup		X	X	X	PR.IP, PR.PO-P	PR.IP-4, PR.PO-P3
CP-09(01)	System Backup | Testing for Reliability and Integrity			X	X	PR.IP, PR.PO-P	PR.IP-4, PR.PO-P3

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
CP-09(02)	System Backup | Test Restoration Using Sampling				X	PR.IP, PR.PO-P	PR.IP-4, PR.PO-P3
CP-09(03)	System Backup | Separate Storage for Critical Information				X	PR.IP, PR.PO-P	PR.IP-4, PR.PO-P3
CP-09(05)	System Backup | Transfer to Alternate Storage Site				X	PR.IP, PR.PO-P	PR.IP-4, PR.PO-P3
CP-09(06)	System Backup | Redundant Secondary System					PR.IP, PR.PO-P	PR.IP-4, PR.PO-P3
CP-09(07)	System Backup | Dual Authorization					PR.IP, PR.PO-P	PR.IP-4, PR.PO-P3
CP-09(08)	System Backup | Cryptographic Protection			X	X	PR.IP, PR.PO-P	PR.IP-4, PR.PO-P3
CP-10	System Recovery and Reconstitution		X	X	X	PR.IP, RS.RP, RC.RP, PR.PO-P	PR.IP-9, RS.RP-1, RC.RP-1, PR.PO-P7
CP-10(02)	System Recovery and Reconstitution | Transaction Recovery			X	X	PR.IP, RS.RP, RC.RP, PR.PO-P	PR.IP-9, RS.RP-1, RC.RP-1, PR.PO-P7
CP-10(04)	System Recovery and Reconstitution | Restore Within Time Period				X	PR.IP, RS.RP, RC.RP, PR.PO-P	PR.IP-9, RS.RP-1, RC.RP-1, PR.PO-P7
CP-10(06)	System Recovery and Reconstitution | Component Protection					PR.IP, RS.RP, RC.RP, PR.PO-P	PR.IP-9, RS.RP-1, RC.RP-1, PR.PO-P7
CP-11	Alternate Communications Protocols					ID.BE, PR.PT, PR.PT-P	ID.BE-5, PR.PT-5, PR.PT-P4
CP-12	Safe Mode					PR.PT, PR.PT-P	PR.PT-5, PR.PT-P4
CP-13	Alternative Security Mechanisms					PR.PT, PR.PT-P	PR.PT-5, PR.PT-P4