Information Technology (IT) Incident Response (IR) Standard

January 31, 2022

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: 2022.02.11 11:45:33 -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 NIST guidance issued to comply with the EO.
1.2	2/11/2022	Update Control Overlay IR-3 ED-01 and Control Overlay IR-8 ED-01.

Table of Contents

1 INTRODUCTION

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 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 baseline information system controls.

This governance document establishes Department information technology (IT) system incident response 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, Binding Operational Directives, and Department Administrative Communications System (ACS) directives and policies. In doing so, these standards supersede any prior governance documentation establishing such standards.

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 incident response control standards.

2 STANDARDS

The Department standards for IT Incident Response 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 199 categorization level (e.g., Low (L), Moderate (M) and High (H)) is assigned to each requirement. This designator indicates a

[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/sites/whitehouse.gov/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

requirement applies to information systems categorized at that FIPS 199 impact-level. Designators are also used to indicate when NIST SP 800-53 Privacy (P) baseline controls 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 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 Overlay issued and maintained by the Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA).

This standard directly supports the Department's integration of the NIST Cyber Security Framework (CSF) in focusing on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the Department's risk management processes. Refer to Appendix A for a summary of controls by baseline and corresponding NIST CSF categories and subcategories.

2.1 IR-1 Policy and Procedures (P, 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 OCIO: 3-112/ACSD-OCIO-004, *Cybersecurity Policy* a Department-level IT Incident Response 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 OCIO: 3-112/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 Incident Response 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 Incident Response policy and the associated controls. The ISO and ISSO shall review Incident Response 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 IR-2 Incident Response Training (P, L, M, H and Control Overlay)

a. Provide incident response training consistent with assigned roles and responsibilities:
    1. Within thirty (30) days of assuming an incident response role or responsibility or acquiring system access.
    2. When required by system changes; and
    3. Annual refresher training thereafter
b. Review and update incident response training content at least annually (i.e., each fiscal year) and following events that may precipitate an update to incident response training content including, but not limited to:
    1. An incident response plan testing or response to an actual incident, to incorporate lessons learned.
    2. Assessment or audit findings; or
    3. Changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Control Overlay IR-2 ED-01 (L, M, H): Train all security operations personnel and incident response team members, based on their roles and responsibilities, on how to handle incidents involving Executive Order (EO)-critical software or EO-critical software platforms.

2.2.1 IR-2(1) Incident Response Training | Simulated Events (H)

Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.

2.2.2 IR-2(2) Incident Response Training | Automated Training Environments (H)

Provide an incident response approved training environment using ED approved interactive simulations based on real-world data.

2.2.3 IR-2(3) Incident Response Training | Breach (P)

Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.

2.3 IR-3 Incident Response Testing (P, M, H and Control Overlay)

Test the effectiveness of the incident response capability for the system at least annually (i.e., each fiscal year) using the following tests:

a. Tabletop or functional tests/checklist;

b. Strategic and tactical threat modeling;

c. Simulations;

d. Ad hoc penetration assessments; and

e. Other assessment methods identified and authorized by the Department.

Control Overlay IR-3 ED-01 (L, M, H): Use the current version of the IRP to document results of annual incident response plan testing. Cloud service providers and Shared Services are not required to upload testing artifacts into CSAM but are required to document testing dates in CSAM.

2.3.1 IR-3(2) Incident Response Testing | Coordination with Related Plans (M, H)

Coordinate incident response testing with organizational elements responsible for related plans.

2.4 IR-4 Incident Handling (P, L, M, H)

a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.

b. Coordinate incident handling activities with contingency planning activities.

c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.

d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

2.4.1 IR-4(1) Incident Handling | Automated Incident Handling Processes (M, H)

Support the incident handling process using EDSOC automated mechanisms.

2.4.2 IR-4(4) Incident Handling | Information Correlation (H)

Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

2.4.3 IR-4(11) Incident Handling | Integrated Incident Response Team (H)

Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in 30 days or less based upon availability of staffing, funding and tools.

2.5 IR-5 Incident Monitoring (P, L, M, H)

Track and document incidents.

2.5.1 IR-5(1) Incident Monitoring | Automated Tracking, Data Collection, and Analysis (H)

Track incidents and collect and analyze incident information using methodology within the Incident Response Plan (IRP).

2.6 IR-6 Incident Reporting (P, L, M, H and Control Overlay)

a. Require personnel to report suspected incidents to the organizational incident response capability immediately and without unreasonable delay.

b. Report incident information to the EDSOC and ISSO.

Control Overlay IR-6 ED-01 (L, M, H): Specify timelines in accordance with the current version of NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* for public and internal incident notification timelines.

Control Overlay IR-6 ED-02 (L, M, H): Report incidents that may constitute a computer crime (violations of applicable Federal and/or State laws) to the Office of the Inspector General (OIG). Appendix B: Reportable Events provides examples of incident types which must be reported.

2.6.1 IR-6(1) Incident Reporting | Automated Reporting (M, H)

Report incidents using ED approved automated mechanisms.

2.6.2 IR-6(3) Incident Reporting | Supply Chain Coordination (M, H)

Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

2.7 IR-7 Incident Response Assistance (P, L, M, H)

Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.

2.7.1 IR-7(1) Incident Response Assistance | Automation Support for Availability of Information and Support (M, H)

Increase the availability of incident response information and support using ED approved automated mechanisms.

2.8 IR-8 Incident Response Plan (IRP) (P, L, M, H and Control Overlay)

a. Develop an incident response plan that:

1. Provides the organization with a roadmap for implementing its incident response capability; Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;
2. Describes the structure and organization of the incident response capability;
3. Provides a high-level approach for how the incident response capability fits into the overall organization;
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;
6. Provides metrics for measuring the incident response capability within the organization;
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;
8. Addresses the sharing of incident information;
9. Is reviewed and approved by personnel responsible for SSP approval in accordance with the Department's required authorization documentation standards; and
10. Explicitly designates responsibility for incident response to EDSOC.

b. Distribute copies of the incident response plan to ISO, ISSO, and system personnel with incident response responsibilities;

c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;

d. Communicate incident response plan changes to ISO, ISSO and system personnel with incident response responsibilities; and

e. Protect the incident response plan from unauthorized disclosure and modification.

Control Overlay IR-8 ED-01 (L, M, H): Use the current version of the authorized IRP template to develop system level plans; use of these templates is not required for cloud service providers and Shared Services.

2.8.1 IR-8(1) Incident Response Plan | Breaches (P)

Include the following in the Incident Response Plan for breaches involving personally identifiable information:

a. A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;

b. An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and

c. Identification of applicable privacy requirements.

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

ACS	Administrative Communications System
AO	Authorizing Official
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CSF	Cybersecurity Framework
DoS	Denial of Service
DHS	Department of Homeland Security
ED	Department of Education
EO	Executive Order
EDSOC	ED Security Operations Center
FIPS	Federal Information Processing Standard
IAS	Information Assurance Services
IRP	Incident Response Plan
ISO	Information System Owner
ISSO	Information Systems Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
PII	Personally Identifiable Information
PO	Principal Office
RAF	Risk Acceptance Form
SAOP	Senior Agency Official for Privacy

5 APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY

The applicability for each baseline control parameter is shown below. NIST SP 800-53 controls that are not applicable to any control baseline are shaded in gray.

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
IR-1	Policy and Procedures	x	x	x	x	PR.IP, DE.DP, GV.PO-P, GV.MT-P, CM.AW-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, CM.AW-P7, PR.PO-P7
IR-2	Incident Response Training	x	x	x	x	PR.AT, GV.AT-P, CM.AW-P	PR.AT-5, GV.AT-P3, CM.AW-P7
IR-2(1)	Incident Response Training | Simulated Events				x	PR.AT, GV.AT-P, CM.AW-P	PR.AT-5, GV.AT-P3, CM.AW-P7
IR-2(2)	Incident Response Training | Automated Training Environments				x	PR.AT, GV.AT-P, CM.AW-P	PR.AT-5, GV.AT-P3, CM.AW-P7
IR-2(3)	Incident Response Training | Breach	x				PR.AT, GV.AT-P, CM.AW-P	PR.AT-5, GV.AT-P3, CM.AW-P7
IR-3	Incident Response Testing	x		x	x	ID.SC, PR.IP, RS.CO, PR.PO-P	ID.SC-5, PR.IP-7, PR.IP-10, RS.CO-1, PR.PO-P5, PR.PO-P8
IR-3(1)	Incident Response Testing | Automated Testing					ID.SC, PR.IP, RS.CO, PR.PO-P	ID.SC-5, PR.IP-7, PR.IP-10, RS.CO-1, PR.PO-P5, PR.PO-P8
IR-3(2)	Incident Response Testing | Coordination with Related Plans			x	x	ID.SC, PR.IP, RS.CO, PR.PO-P	ID.SC-5, PR.IP-7, PR.IP-10, RS.CO-1, PR.PO-P5, PR.PO-P8
IR-3(3)	Incident Response Testing | Continuous Improvement					ID.SC, PR.IP, RS.CO, PR.PO-P	ID.SC-5, PR.IP-7, PR.IP-10, RS.CO-1, PR.PO-P5, PR.PO-P8
IR-4	Incident Handling	x	x	x	x	ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2,

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.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-4(1)	Incident Handling | Automated Incident Handling Processes			x	x	ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-4(2)	Incident Handling | Dynamic Reconfiguration					ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7

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
IR-4(3)	Incident Handling | Continuity of Operations					ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-4(4)	Incident Handling | Information Correlation				x	ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-4(5)	Incident Handling | Automatic Disabling of System					ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1,

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
							RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-4(6)	Incident Handling | Insider Threats					ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-4(7)	Incident Handling | Insider Threats — Intra-organization Coordination					ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-4(8)	Incident Handling | Correlation with External Organizations					ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO,	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3,

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
						GV.MT-P, CM.AW-P	RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-4(9)	Incident Handling | Dynamic Response Capability					ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-4(10)	Incident Handling | Supply Chain Coordination					ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7

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
IR-4(11)	Incident Handling | Integrated Incident Response Team				x	ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-4(12)	Incident Handling | Malicious Code and Forensic Analysis					ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-4(13)	Incident Handling | Behavior Analysis					ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1,

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
							RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-4(14)	Incident Handling | Security Operations Center					ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-5	Incident Monitoring	x	x	x	x	ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-5(1)	Incident Monitoring | Automated Tracking, Data Collection, and Analysis				x	DE.AE, RS.AN	DE.AE-3, DE.AE-5, RS.AN-1, RS.AN-4

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
IR-6	Incident Reporting	x	x	x	x	DE.AE, RS.AN	DE.AE-3, DE.AE-5, RS.AN-1, RS.AN-4
IR-6(1)	Incident Reporting | Automated Reporting			x	x	RS.CO, CM.AW-P	RS.CO-2, CM.AW-P7
IR-6(2)	Incident Reporting | Vulnerabilities Related to Incidents					RS.CO, CM.AW-P	RS.CO-2, CM.AW-P7
IR-6(3)	Incident Reporting | Supply Chain Coordination			x	x	RS.CO, CM.AW-P	RS.CO-2, CM.AW-P7
IR-7	Incident Response Assistance	x	x	x	x	RS.CO, CM.AW-P	RS.CO-2, CM.AW-P7
IR-7(1)	Incident Response Assistance | Automation Support for Availability of Information and Support			x	x	PR.IP, CM.AW-P, PR.PO-P	PR.IP-9, CM.AW-P8, PR.PO-P7
IR-7(2)	Incident Response Assistance | Coordination with External Providers					PR.IP, CM.AW-P, PR.PO-P	PR.IP-9, CM.AW-P8, PR.PO-P7
IR-8	Incident Response Plan	x	x	x	x	PR.IP, CM.AW-P, PR.PO-P	PR.IP-9, CM.AW-P8, PR.PO-P7
IR-8(1)	Incident Response Plan | Breaches	x				ID.SC, PR.IP, DE.AE, RS.RP, RS.CO, RS.AN, RS.IM, RC.RP, RC.IM, CM.AW-P, PR.PO-P	ID.SC-5, PR.IP-7, PR.IP-8, PR.IP-9, DE.AE-3, DE.AE-5, RS.RP-1, RS.CO-1, RS.CO-2, RS.CO-3, RS.CO-4, RS.AN-4, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, CM.AW-P7, PR.PO-P5, PR.PO-P6, PR.PO-P7
IR-9	Information Spillage Response					ID.SC, PR.IP, DE.AE, RS.RP, RS.CO, RS.AN, RS.IM, RC.RP, RC.IM, CM.AW-P, PR.PO-P	ID.SC-5, PR.IP-7, PR.IP-8, PR.IP-9, DE.AE-3, DE.AE-5, RS.RP-1, RS.CO-1, RS.CO-2, RS.CO-3, RS.CO-4, RS.AN-4, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, CM.AW-P7, PR.PO-P5, PR.PO-P6, PR.PO-P7

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
IR-9(2)	Information Spillage Response | Training					ID.SC, PR.IP, PR.PO-P	ID.SC-5, PR.IP-9, PR.PO-P7
IR-9(3)	Information Spillage Response | Post-spill Operations					ID.SC, PR.IP, PR.PO-P	ID.SC-5, PR.IP-9, PR.PO-P7
IR-9(4)	Information Spillage Response | Exposure to Unauthorized Personnel					ID.SC, PR.IP, PR.PO-P	ID.SC-5, PR.IP-9, PR.PO-P7

6 APPENDIX B – REPORTABLE EVENTS

Incidents that may constitute a computer crime (violations of applicable Federal and/or State laws) must be reported to the OIG. Examples of the types of incidents that must be reported include, but are not limited to, the following:

Description	Example
Reportable Events to OIG	
Denial of Service (DoS)	CISA reports of DoS attacks on ED systems. Examples of DoS include, Buffer Overflow, ICMP Floor, and SYN Flood attempts.
Unauthorized Access on internally and externally hosted systems, as well as FSA partner systems	Individuals intentionally trying to gain access to PII information, systems, or components that they do not authorization to access.
Exceeding authorized access (abuse of system privileges)	A system user uses his or her privileges to conduct unauthorized searches for loan information.
Criminal misuse of information technology (IT) resources	An employee who uses his or her government issued equipment to operate a business on government time and government laptop. Additional activities include, fraud, theft, hacking, and identify theft.
Illegal interception of electronic communications	An individual who set themselves up as proxy or delegate to get access to an executive's email account without their knowledge. The use of any electronic, mechanical, or other device to intercept communications transmitted by wire, cable, or radio, e.g., Man-in-the-Middle, unauthorized port mirroring/packet capture, and unauthorized proxies or Wi-Fi hotspots with the intention of intercepting end-user traffic
Compromise of System or Application privileges (root access)	An external threat actor compromises an admin/root account on a system or application.
Compromise of information protected by law	During contract negotiations, a Department employee or contractor sends non-releasable contract or bid related information to their private, or their company, email address.

Description	Example
	When an employee's misconduct or administrative investigation (involving one or more employees) is being reviewed by management, and an individual then releases that information to the press or media without authorization
Attempts to access child pornography	An individual is found to be accessing child pornography using Department systems.
Malicious destruction or modification of Department data and/or information	An example is when an individual is found to be maliciously deleting or modifying Department data without proper authorization, including Department data hosted at external partner systems (e.g., Servicers, Title IVs, and Schools).
Non-Reportable Events to OIG	
Unauthorized Disclosure	A user accidentally sends an email of another individual's SSN to the wrong email address. The user then self-reports the event to EDSOC. A user self-reports finding an unprotected document, configured without the proper security permissions, containing PII, such as Social Security numbers. The user informs EDSOC of his or her discovery. EDSOC conducts a review and determines only authorized users have access to the file.