	Department of Human Services Online Directives Information System	Index: Revised: Next Review:	POL1906 01/05/2022 01/05/2024

SUBJECT: DHS Information Security Policies

Incident Response and Reporting

Policy
To establish and implement policies and procedures to ensure proper incident response and reporting for DHS information systems. The objective of this policy is to address the considerations that will help to ensure that the DHS IT resources and information systems properly respond to and report incidents concerning DHS information systems and data. Critical to achieving this objective is the implementation of controls that address each of the requirements stated in this policy.

Authority

1. United States Department of Commerce National Institute for Standards and Technology (NIST)
2. United States Internal Revenue Service
3. United States Department of Health & Human Services
4. Centers for Medicare & Medicaid Services
5. Georgia Technology Authority

References:

- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, January 2015
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-61 Computer Incident Handling Guide Revision 2 August 2012
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops Revision 1 July 2013
- United States Internal Revenue Service, IRS Publication 1075 Tax Information Security Guidelines For Federal, State and Local Agencies Safeguards for Protecting Federal Tax Returns and Return Information

Purpose
This policy establishes the DHS Information Security Incident Management Policy. This policy is designed to support risk mitigation activities that stem from computer security incidents, by establishing of an Enterprise Incident Response capability. The incident management program is one of four key agency IT security practices that is used to detect, analyze, prioritize and handle Cyber Security Incidents which may occur within DHS.

Scope

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by DHS. Any information not specifically identified as the property of other parties, that is transmitted or stored on DHS IT resources (including e-mail, messages and files) is the property of DHS. All users (DHS employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

Responsibilities

DHS shall adopt the Incident Management principles established in the National Institute for Standards and Technology (NIST) Special Publication (SP) 800-61 "Computer Security Incident Handling Guide," as the official policy for Incident Response. The following subsections outline the incident management standards that constitute DHS policy. Each DHS Business System is then bound to this policy, and shall develop or adhere to a program plan which demonstrates compliance with the policy related the standards documented.

- **IR-1 Incident Response Policies and Procedures**
    1. Senior management, management, and all organization entities are required to coordinate and implement necessary controls for conducting incident response and reporting policy and procedures for IT resources and information systems on the basis of business and security requirements.
    2. Periodic reviews of this shall be performed and documented at least within every **three years**, or when there is a **significant change**.
    3. Periodic review of incident response and reporting procedures shall be performed at least **annually**.
- **IR-2 Incident Response Training**
  DHS provides incident response training consistent with assigned roles and responsibilities to information system users:
    1. Within **ninety** (90) days of assuming an incident response role or responsibility.
    2. When required by information system changes.
    3. Within every **three hundred sixty-five** (365) days thereafter.
- **IR-3 Incident Response Testing and Exercise**
    1. DHS tests the incident response plan at least **annually.**
    2. Tabletop exercises are performed which test the agency's incident response policies and procedures. Scenarios that include a breach of FTI data are included in these exercises.
    3. Each tabletop exercise produces an after-action report to improve existing processes, procedures, and policies.
    4. DHS develops, reviews, and updates agency-level IR Test Plans, and updates incident response plans annually.
    5. IR Plan weaknesses are identified and remediated using the results of incident response tests/exercises.
    6. Corrective actions are captured in the Plan of Action and Milestones (POA&M) for the particular information system.

- **IR-4 Incident Handling**
    1. Incident handling procedures are utilized which possess the capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery
    2. Incident handling activities are coordinated with contingency planning activities
    3. Lessons learned are incorporated from ongoing incident handling activities into incident

- **IR-5 Incident Monitoring**
  DHS has developed and adheres to our documented incident monitoring processes which track and document information system security incidents on an ongoing basis. Tracked items include security incidents potentially affecting the confidentiality of FTI.
- **IR-6 Incident Reporting**
    1. The agency reports all identified Information Security Incidents to the DHS Office of Technology Information Security division upon discovery of the incident.
    2. If an incident involves FTI, the agency contacts the appropriate special agent-in-charge, TIGTA, and the IRS Office of Safeguards immediately but no later than 24 hours after identification of a possible issue involving FTI.
- **IR-7 Incident Response Assistance**
  DHS maintains and provides incident response resources to the agency which offer advice and assistance to users of agency information systems for handling and reporting security incidents.
- **IR-8 Incident Response Plan**
    1. DHS maintains an agency approved incident response plan that:
        a) Provides the agency with a roadmap for implementing its incident response capability.
        b) Describes the structure of the incident response capability.
        c) Provides a high-level approach for how the incident response capability fits into the overall agency.
        d) Meets the unique requirements of the agency, which relate to mission, size, structure, and functions
        e) Defines reportable incidents
        f) Provides metrics for measuring the incident response capability within the agency
        g) Defines the resources and management support needed to effectively maintain and mature an incident response capability
        h) Is reviewed and approved by designated agency officials
    2. Copies of the incident response plan are distributed to authorized incident response personnel.
    3. The incident response plan is reviewed, at a minimum, on annually, or as an after-action review. It is updated to address system/agency changes or problems encountered during plan implementation, execution, or testing.
    4. Incident response plan changes are communicated and disseminated to authorized incident response personnel upon change updates during discussion,

documentation, and finalization phases of update periods.

5. The incident response plan is protected from unauthorized disclosure and modification via implemented access control mechanisms.

- **IR-9 Information Spillage Response**

1. **For FTI Data:** Upon discovering a possible improper inspection or disclosure of FTI, including breaches and security incidents, by a federal employee, a state employee, or any other person, the individual making the observation or receiving information must contact the office of the appropriate special agent-in-charge, TIGTA immediately, but no later than 24 hours after identification of a possible issue involving FTI. Call the local TIGTA Field Division Office first.

   If unable to contact the local TIGTA Field Division, contact the Hotline Number.
   Hotline Number: 800-589-3718
   TIGTA Homepage: https://www.treasury.gov/tigta
   Mailing Address: Treasury Inspector General for Tax Administration
   Ben Franklin Station
   P.O. Box 589
   Washington, DC 20044-0589

   Concurrent to notifying TIGTA, the agency must notify the Office of Safeguards by email to Safeguards mailbox, safeguardreports@irs.gov. To notify the Office of Safeguards, the agency must document the specifics of the incident known at that time into a data incident report, including but not limited to:
   a) Name of agency and agency Point of Contact for resolving data incident with contact information
   b) Date and time the incident occurred
   c) Date and time the incident was discovered
   d) How the incident was discovered
   e) Description of the incident and the data involved, including specific data elements, if known
   f) Potential number of FTI records involved; if unknown, provide a range if possible
   g) Address where the incident occurred
   h) IT involved (e.g., laptop, server, mainframe)

- Reports must be sent electronically and encrypted via IRS-approved encryption techniques. Use the term data incident report in the subject line of the email. Do not include any FTI in the data Incident report.
- Even if all information is not available, immediate notification is the most important factor, not the completeness of the data incident report. Additional information must be provided to the Office of Safeguards as soon as it is available.
- The agency will cooperate with TIGTA and Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident.
- The agency must not wait to conduct an internal investigation to determine if FTI was involved in an unauthorized disclosure or data breach. If FTI may have been involved, the agency must contact TIGTA and the IRS immediately.
- Incident response policies and procedures required in *Section 10.0, Reporting Improper Inspections or Disclosures*, of IRS Publication 1075 must be used when responding to an identified unauthorized disclosure or data breach incident.

- The Office of Safeguards will coordinate with the agency regarding appropriate follow- up actions required to be taken by the agency to ensure continued protection of FTI.

Once the incident has been addressed, the agency will conduct a post-incident review to ensure the incident response policies and procedures provide adequate guidance. Any identified deficiencies in the incident response policies and procedures should be resolved immediately. Additional training on any changes to the incident response policies and procedures should be provided to all employees, including contractors and consolidated data center employees, immediately.

2. **FOR SOCIAL SECURITY ADMINISTRATION DATA**
   If the agency suspect a breach or loss of PII, or a security incident which includes SSA- provided data, they must notify the United States Computer Emergency Readiness Team (US-CERT) **within one hour** of discovering the incident. The agency must also notify the SSA Systems Security contact named in the agreement. If within 1 hour the agency has been unable to make contact with that person, the agency must call the SSA's Network Customer Service Center (NCSC) toll free at 877-697-4889 (select "Security and PII Reporting" from the options list). Agency personnel will provide updates as they become available to the SSA contact, as appropriate.

Incident Response Notification to Impacted Individuals

- Notification to impacted individuals regarding an unauthorized disclosure or data breach incident is based upon the agency's internal incident response policy since the FTI is within the agency's possession or control.
- However, the agency must inform the Office of Safeguards of notification activities undertaken before release to the impacted individuals. In addition, the agency must inform the Office of Safeguards of any pending media releases, including sharing the text, prior to distribution.

FTI Suspension, Termination, and Administrative Review

- The federal tax regulation 26 CFR 301.6103(p)(7)-1 establishes a process for the suspension or termination of FTI and an administrative review if an authorized recipient has failed to safeguard returns or return information. For more information, refer to *Exhibit 3, U.S.C Title 26, CFR 301.6103(p)(7)-1.*

All incident response, reporting, and escalation procedures shall be formally documented and approved by the DHS Chief Information Officer / DHS Chief Information Security Officer.

History
None

The Office of Information Technology (OIT), upon recommendation of the DHS Chief Information Security Officer (CISO), evaluates this policy annually by:

1. Comparing its content and intent to evolving regulatory compliance standards imposed upon the Agency, such as, IRS 1075, NIST 800-53, and CMS MARS-E.
2. Addressing any deficiencies or gaps discovered during periodic audits conducted by Georgia DOAA or other regulatory bodies, such as, IRS, CMS, SSA, FBI, etc.