Paperwork Reduction Act

Privacy Act Notice

PURPOSE: The Incident Reporting Form enables U.S. Federal Government agencies and external entities to report security incidents under investigation to the Cybersecurity and Infrastructure Security Agency (CISA). The information is used by CISA to provide appropriate responses to affected entities and to gain greater insights into security threats.

Incident Reporting Form

Current Content Requested on CISA Reporting Form
https://www.cisa.gov/forms/report

What is an incident?
For the federal government, incident, as defined by the Federal Information Security Modernization Act of 2014 (44 USC 3552), means an occurrence that-

(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

(B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Federal incident notification guidelines, including definitions and reporting timeframes can be found at https://www.cisa.gov/federal-incident-notification-guidelines.

In general, types of activity that may qualify as an incident include but are not limited to:

- *network intrusions that gain unauthorized access to a system or its data, including Personally Identifiable Information (PII) related incidents*
- *malicious disruption or denial of service*
- *the unauthorized use of a system for modifying data*

- *changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent*

We encourage you to report any activities that you feel meet the definition of an incident.

Using the CISA Incident Reporting System
In order for us to respond appropriately, please answer the questions as completely and accurately as possible. Questions that must be answered are marked with a red asterisk. This website uses Transport Layer Security (TLS) to provide more secure communications than unencrypted email.

Do not copy and paste malicious code directly into this form. Fill out this incident report in detail. Then, provide the resulting CISA Incident ID number in the Open Incident ID field of the Malware Analysis Submission Form where you can submit a file containing the malicious code.

Please refrain from including PII or SPII in incident submissions unless the information is necessary to understanding the nature of the cybersecurity incident.

Do not copy and paste malicious code directly into this form. Fill out this incident report in detail. Then, provide the resulting CISA Incident ID number in the Open Incident ID field of the Malware Analysis Submission Form where you can submit a file containing the malicious code.

** Required fields for all reports*[1]

Select One*:
I am: [ ] the impacted user
[ ] reporting on behalf of the impacted user

1. Your Contact Info
   - First Name
   - Last Name
   - Telephone
   - Email Address*

[ ] I would like to report the impacted user's contact information and have the individual's consent to do so.
Impacted User's Contact Information
   - First Name
   - Last Name
   - Telephone
   - Email Address* (NOTE: This is a required field but only if the checkbox in above question is activated and the "reporting on behalf of the impacted user" option is selected.)

[1] "Required" here only means the responses technically necessary to submit the incident on CISA's incident reporting form.

Select One of the three options below*:
[ ] I am reporting for a Federal Government agency to the Cybersecurity and Infrastructure Security Agency (CISA) under the Federal Information Security Modernization Act of 2014 (FISMA 2014)

[ ] I am voluntarily reporting (Select this option only if you are not reporting to satisfy a requirement to file an incident report)

[ ] I am reporting to CISA to satisfy a regulatory, statutory, and/or contractual requirement (other than FISMA 2014). You must indicate the specific requirement below to tell us you are reporting under that requirement. Note that the options are organized based on the agency or organization that issues/oversees the applicable reporting requirement. We will share your report with the entity you select in accordance with the arrangements in place at the time of reporting.

DISPLAY NOTE: ***"To the extent a reporting requirement provides that reporting to CISA is a means of compliance, you must indicate the specific requirement below to be considered as reporting under that requirement."***

(DESIGN NOTE: If this option is selected, present the reporter the list below and allow a multi select)

Please select the reporting requirement from the options below:

A. Federal Energy Regulatory Commission (FERC)/ North American Electric Reliability Corporation (NERC)
    1. Critical Infrastructure Protection Reliability Standards CIP-003-8 (Cyber Security Management Controls) and CIP008-6 (Cyber Security – Incident Reporting and Response Planning)
B. Federal Risk and Authorization Management Program (FedRAMP)
C. Nuclear Regulatory Commission
    1. Cyber security event notifications (10 C.F.R 73.77)
D. Transportation Security Administration (TSA)
    1. Security Directives or Information Circulars associated with Freight Rail, Public Transportation and Passenger Railroad Cybersecurity
    2. Security Directives or Information Circulars associated with Pipeline Cybersecurity
    3. Security Directives or Information Circulars associated with Aviation Cybersecurity, including directives or circulars for:
        a. Airport Security Program (ASP),
        b. Aircraft Operator Standard Security Program (AOSSP),
        c. Full All-Cargo Aircraft Operator Standard Security Program (FACAOSSP),
        d. Twelve-Five Standard Security Program (TFSSP),
        e. Private Charter Standard Security Program (PCSSP),
        f. Indirect Air Carrier Standard Security Program (IACSSP),
        g. Certified Cargo Screening Standard Security Program (CCSSP)

h. Other

E. Reserved
   1. Reserved

F. Other (option to select more than one entry pair if applicable)
   1. Regulator (Please describe the regulator)
      a. Regulation (Please describe the regulation(s) associated with this regulator) (Option to add more than one regulation per regulator)

2. Organization Details **(DESIGN NOTE: If report is identified as a FISMA report, U.S. Fed Gov shall be the only option presented to the reporter to further identify which agency/sub-agency they belong to. All other reports will not have the U.S. Gov option to select from)**

- What type of organization are you reporting for? *(select one from the following options)*
  - Critical Infrastructure and/or Private Sector
    - Please enter your organization or company name *(please spell out any acronyms):*
    - Please select the primary Critical Infrastructure sector in your organization or company that is involved and impacted by this incident: *(select from a drop-down menu).*
      - Optional: which critical infrastructure sub-sector you belong to *(select from a drop-down menu).* (**DISPLAY NOTE**: ***Sub-sectors listed are available depending on the critical infrastructure you select***)
  - United Stated Federal Government **(DESIGN NOTE: If report is identified as a FISMA report, this shall be the only option presented to the reporter to further identify which agency/sub-agency they belong to)**
    - Please select what federal agency you are affiliated with *(select from a drop-down menu).*
    - Please select what federal sub-agency you are affiliated with *(select from a drop-down menu).* (**DISPLAY NOTE**: ***Sub-agencies listed are available depending on the agency you select***)
  - Foreign Government
    - If you are a Foreign Government, you are required to select from a drop down menu the country in which you are located.
    - A second optional question asks if your organization is a national CSIRT.
  - U.S. State, Local, Territorial, or Tribal (SLTT) Government
    - If you are an SLTT entity, you must select your state and
    - You must enter your SLTT organization name
  - Information Sharing and Analysis Center (ISAC)
    - If you are an ISAC, you are required to select from a drop down menu which subagency (i.e., ISAC) you belong to
  - I am an Individual, not an organization.
- Please enter your organization's internal tracking number *(if applicable)*

3. Incident Description*
- When, approximately, did the incident start?
- When was this incident detected/identified?*

- From what time zone are you making this report?
- Please enter a brief description of the incident.*

4. Impact Details

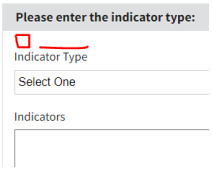
System Impact

- Please define the functional impact to the organization *(select one)*:*
  - No impact
  - No impact to services
  - Minimal impact to non-critical services
  - Minimal impact to critical services
  - Significant impact to non-critical services
  - Denial of non-critical services
  - Significant impact to critical services
  - Denial of critical services or loss of control
- What is the number of systems impacted?*
- How many users are impacted?*
- How was this incident detected?**(select one or more of the following)*
  - Administrator
  - Anti-Virus Software
  - Intrusion Detection System (IDS)
  - Log Review
  - User
  - Unknown
  - Other
- What operating systems (OS) are impacted? *(can include as many as necessary)*
  - OS Name
  - OS Version
- What is the function of the system(s) affected? *Please select all that apply:*
  - Application Server(s)
  - Database Server(s)
  - Desktop(s)
  - Domain Name Server(s)
  - Firewall(s)
  - ICS/SCADA System(s)
  - Laptop(s)
  - Mail Server(s)
  - Router(s)
  - Switch(es)
  - Time Server(s)
  - Web Server(s)
  - Other Server(s)

[ ] The information contained in this submission should be considered commercial, financial, and proprietary under the Cybersecurity Information Sharing Act of 2015

(DISPLAY NOTE: ***"If selected, at least one indicator type, indicator value, and context must be populated")***

(DESIGN NOTES: Not Presented for FISMA reports. If CISA 2015 box is checked, at least one indicator type, indicator value, and context must be populated. If not, the system must present an error to the user and prevent the submission of the incident. Placed within the "Indicator" box of information.)



- Please select the indicator type *(from the drop down menu)* and, for each one selected, provide information on the Indicators and the Indicator Context. You can do this for as many indicator types as applicable. The drop down menu of types are:
  - Network – Autonomous System(s) (AS)
  - Network – Domain Name(s)
  - Network – Email Address(es)
  - Network – Email Message(s)
  - Network – IPv4 Address(es)
  - Network – IPv6 Address(es)
  - Network – Network Traffic
  - Network – URL
  - Host – File System Directory(ies)
  - Host – File meta-data
  - Host – Hash(es)
  - Host – Mutex(es)
  - Host – Software meta-data
  - Host – System Processes
  - Host – User Account(s)
  - Host – Windows Registry
  - Host – X 509 Certificate(s)
- Enter Common Vulnerabilities and Exposures Identifiers (CVE-ID). Please do not include the CVE prefix (e.g., 2014-7654321)

Observed Activity

- Where was the activity observed?* *(select one)*
  - Level 1 – Business DMZ
  - Level 2 – Business Network
  - Level 3 – Business Network Management
  - Level 4 – Critical System DMZ
  - Level 5 – Critical System Management
  - Level 6 – Critical Systems
  - Level 7 – Safety Systems
  - Unknown
- Please characterize the observed activity at its most severe level.* *(select one)*
  - None
  - Preparation
  - Engagement
  - Presence

- Effect/Consequence

Information Impact

- What is the known informational impact from the incident?* *(select one)*
  - No impact
  - Suspected but not identified
  - Privacy Data Breach, within the scope of OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information"

    (DESIGN NOTE: If "Privacy Data Breach is selected, then additional questions are asked)
    - Number of individuals whose Personally Identifiable Information (PII) was accessed or exfiltrated: *Number* *
    - What type(s) of PII was accessed or exfiltrated? *Choose all that apply*:
      - Biometrics
      - Contact information
      - Financial
      - Federal employee personnel
      - Federal unique identifiers
      - Interactions with agency
      - Medical
    - Is the reporting agency (or another entity) providing notifications to individuals whose PII was accessed or exfiltrated?
      - Yes
      - No
    - If the reporting agency (or another entity) is providing services to individuals whose PII was accessed or exfiltrated, please enter the number of individuals provided the following services
      - Identity Monitoring: Number
      - Credit Monitoring: Number
      - Identity Theft Insurance: Number
      - Full-service identity counseling and remediation services: Number
  - Proprietary Information Breach
  - Destruction of Non-Critical System
  - Critical Systems Data Breach
  - Core Credential Compromise
  - Destruction of Critical System
- Number of records impacted.*

Recovery from Incident

- Please select the organization's recoverability for this incident.* *(select one)*
  - Regular – Time to recovery is predictable with existing resources
    - If selected, submitted is asked to provide estimated recovery time in hours/days and additional details. *Answers to these questions are optional*.

- Supplemented – Time to recovery is predictable with additional resources
  - If selected, submitted is asked to provide estimated recovery time in hours/days, whether or not the organization has identified the additional resources needed, and additional details. Answers to these questions are optional.
- Extended – Time to recovery is unpredictable; additional resources and outside help are needed
  - If selected, submitted is asked to provide whether or not the organization has identified the additional resources needed and additional details. Answers to these questions are optional.
- Non Recoverable – Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly)
  - If selected, submitted is asked to provide additional details. This is optional

==========

DESIGN NOTE: Questions below are conditional to U.S. Federal Government reporting {e.g. FISMA} and NOT subject to PRA.

**These questions are required to be implemented at time of IRP "GO LIVE"
or as soon as the next design iteration and update,
but no later than OMB's PRA renewal approval, currently estimated as 15 Nov 2024.**

The following is NOT dependent upon PRA renewal approval.

==========

(DESIGN NOTE: Additional question depending on if "U.S. Federal Government" is selected)

(DISPLAY NOTE: ***These additional questions below are depending on if "U.S. Federal Government" is selected and support further criteria under FISMA reporting of a major incident and Breach reporting to Congress.)***

Major Incident
(DISPLAY NOTE: ***Please refer to OMB's most current policy for guidance to declare a major incident.)***

Does your agency currently consider this to be a "major incident" per Office of Management and Budget (OMB) guidance? * Required
Yes
No

(DESIGN NOTE: Additional questions depending on if "major incident" selection = "Yes")

You are affirming that your incident is a Major Incident; therefore, this incident is **likely to result in demonstrable harm** to *(Please mark all that apply):*
[ ] National Security Interests,
[ ] Foreign Relations,
[ ] Economy of the United States,
[ ] Public Confidence,
[ ] Civil Liberties, or
[ ] Public health and safety of the American people.

You are affirming that your incident includes a major breach of data, which *(Please mark all that apply):*

[ ] involves personally identifiable information (PII) that was / potentially was, **(DESIGN NOTE: if selected, at least one below must be selection)**

- [ ] exfiltrated,
- [ ] modified,
- [ ] deleted, or
- [ ] otherwise compromised
  - [ ] **and** is **likely to result in demonstrable harm** to the: **(DESIGN NOTE: Only displayed if a PII impact was selected. If this is selected, at least one below must also be selected)**
    - [ ] national security interests,
    - [ ] foreign relations,
    - [ ] economy of the United States,
    - [ ] public confidence, civil liberties, or
    - [ ] public health and safety of the American people

[ ] OR any of the following conditions have occurred to the PII of 100,000 or more people *(Please mark all that apply):* **(DESIGN NOTE: if selected, at least one below must be selected)**

- [ ] unauthorized modification,
- [ ] unauthorized deletion,
- [ ] unauthorized exfiltration,
- [ ] unauthorized access,
- [ ] unauthorized acquisition,
- [ ] loss,
- [ ] theft, or
- [ ] inadvertent disclosure.

(DESIGN NOTE: Additional question depending on if "U.S. Federal Government" AND "Privacy Data Breach" {within Informational Impact} are both selected)

Does your agency currently consider this to be a breach that must be reported to Congress within 30 days in accordance with OMB guidance? * Required

Yes
No