

# CISA INCIDENT REPORTING SYSTEM

SCREENSHOTS

[HTTPS://US-CERT.CISA.GOV/FORMS/REPORT](https://us-cert.cisa.gov/forms/report)

OMB CONTROL NO.: 1670-0037; EXPIRATION DATE: 12/31/2021

# CISA INCIDENT REPORTING SYSTEM INSTRUCTIONS



The screenshot shows the CISA Incident Reporting System website. At the top left is the CISA logo and the text "CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY". To the right is a search bar with a magnifying glass icon and two buttons labeled "Services" and "Report". Below the header is a navigation menu with "Alerts and Tips", "Resources", and "Industrial Control Systems". The main content area features the title "CISA Incident Reporting System" in red, followed by the OMB Control No. and Expiration Date. A paragraph explains the system's purpose and includes a link for "Less Detail". A section titled "What is an incident?" provides a definition and lists types of activities that qualify as incidents, such as network intrusions, denial of service, and unauthorized data modification. The page concludes with an encouragement to report incidents.

**CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY**

Search

Services Report

Alerts and Tips Resources Industrial Control Systems

**CISA Incident Reporting System** OMB Control No.: 1670-0037; Expiration Date: 12/31/2021

The CISA Incident Reporting System provides a secure web-enabled means of reporting computer security incidents to CISA. This system assists analysts in providing timely handling of your security incidents as well as the ability to conduct improved analysis. If you would like to report a computer security incident, please complete the following form. Please provide as much information as you can to answer the following questions to allow CISA to understand your incident. - [Less Detail](#)

**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.us-cert.gov/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.

# INSTRUCTIONS, CONTINUED

## 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 Secure Sockets Layer (SSL) / 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.

Show Pending Required Fields Panel <

Show Malware Submissions Panel <

All fields are optional unless marked \* Required

I am:  the impacted user  reporting on behalf of the impacted user

# CONTACT INFORMATION

## MY CONTACT INFORMATION

---

Please provide your contact information so that we are able to contact you should we need to follow-up. Your contact information is not required to submit a report using this form. However, incomplete contact information may limit US-CERT's ability to process or act on your report.

First Name

Last Name

Telephone

Email Address \* Required

# ORGANIZATION

MY ORGANIZATION

What type of organization are you? \* Required

Private Sector

Please enter your company name:

Please specify either Business or Individual \* Required

Business  Individual

Please enter the organization's internal tracking number (if applicable):

# DATE/TIME OF INCIDENT

## DATE AND TIME INFORMATION

---

When, approximately, did the incident start?

Enter the date using the format YYYY-MM-DD (e.g., 2021-05-21). Enter the time using the format hh:mm:ss (e.g., 21:44:15).

When was this incident detected? \* Required

Enter the date using the format YYYY-MM-DD (e.g., 2021-05-21). Enter the time using the format hh:mm:ss (e.g., 21:44:15).

From what timezone are you making this report?

# INCIDENT DESCRIPTION

**INCIDENT DESCRIPTION**

---

Please enter a brief description of the incident:

**IMPACT DETAILS**

---

Was the confidentiality, integrity, and/or availability of your organization's information systems potentially compromised? \* Required

Yes  No

[Cancel](#) [Next](#)

# PRIVACY ACT STATEMENT

## Privacy Act Statement

**Authority:** 5 U.S.C. § 301 and 44 U.S.C. § 3101 authorize the collection of this information.

**Purpose:** The primary purpose for the collection of this information is to allow the Department of Homeland Security to contact you about your request.

**Routine Uses:** The information collected may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended. This includes using the information as necessary and authorized by the routine uses published in DHS/ALL-002 - Department of Homeland Security (DHS) Mailing and Other Lists System November 25, 2008, 73 FR 71659.


**Disclosure:** Providing this information is voluntary. However, failure to provide this information will prevent DHS from contacting you in the event there are questions about your request.

Version: 3.0 | Report ID: 2021-USCERTv3JJO0Q | Date: 202105212130

[Email comments and feedback on the Incident Reporting Form](#)

### Contact Us

 (888)282-0870

 [Send us email](#)

### Subscribe to Alerts

Receive security alerts, tips, and other updates.

[Report](#)



# PAPERWORK REDUCTION ACT STATEMENT

- CISA estimates that the total average burden per response associated with this collection is approximately 0.05 hours. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid OMB control number. The control number for this collection is OMB 1670-0037, which expires 12/31/2021. Send comments regarding this burden estimate or collection to: DHS/CISA, Attention: PRA 1670-0037, Mailstop: 0635, 245 Murray Lane SW Bldg 410, Washington, DC 20528.