

# CISA INCIDENT REPORTING SYSTEM


SCREENSHOTS

IRF INDEX - IRF

OMB CONTROL NO.: 1670-0037;  
EXPIRATION DATE: 1/31/2028



# SIGN-IN

 **CISA Services Portal**

Report a Cyber Issue ▼ CISA.gov

## CISA Services

CISA provides a secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities. To submit a report, please select a login method below.

### Sign-in

Choose your preferred Login

Sign-In


Report Unregistered


Or


Create an Account

### Don't have an account? Create One!


Once you have an account, you'll have more options when you're reporting an incident.


**Save Your Progress:** Started your report but don't have time to complete it? You can save it to finish later.

**Continue Your Progress:** Pick your report right up again where you left off.

**Track Your Issue:** Once you've submitted an issue, you'll be able to come back to track its progress with CISA.

### Want to Continue Anonymously?

 If you don't wish to share your identity, you're free to [submit your issue anonymously](#) for CISA's review

 Privacy • Terms

# REPORT TO CISA 1 OF 3

## Report to CISA

CISA provides secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities. To submit a report, please select the appropriate method from below:

### Report a Cyber Issue




Report incidents as defined by [NIST Special Publication 800-61 Rev 2](#), to include

- Attempts to gain unauthorized access to a system or its data,
- Unwanted disruption or denial of service, or
- Abuse or misuse of a system or data in violation of policy.

Federal incident notification guidelines, including definitions and reporting timeframes can be found [here](#).

Report Incident

# REPORT TO CISA 2 OF 3

 CISA Services Portal

Report a Cyber Issue ▾ CISA.gov

## Incident Reporting System

OMB Control No.: 1670-0037; Expiration Date: 01/31/2028

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.

CancelStart Incident Reporting Form

### 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

# REPORT TO CISA 3 OF 3

 CISA Services Portal

Report a Cyber Issue ▾ CISA.gov



### 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.


### 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

 **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.

 Privacy - Terms


# REPORT TO CISA

**CISA Services Portal**

Report a Cyber Issue ▼ CISA.gov

### 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

 **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.

The Protected Critical Infrastructure Information (PCII) Program enhances information sharing on the security of critical infrastructure between the public and private sectors with the government by protecting sensitive critical infrastructure information from disclosure per the Critical Infrastructure Information Act of 2002. To learn more visit us at [Protected Critical Infrastructure Information \(PCII\) Program | CISA](#) or email us at [PCII-Assist@mail.cisa.dhs.gov](mailto:PCII-Assist@mail.cisa.dhs.gov).

# 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):

# ORGANIZATION DETAILS

## Organization Details

Required fields are marked with an asterisk (\*).

### The Impacted Organization's Details

What type of organization are you reporting for?\*

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

[Back](#)

[Next](#)

# INCIDENT DESCRIPTION

## Incident Description

Required fields are marked with an asterisk (\*).

### Incident Description

When approximately, did the incident start? \*

mm/dd/yyyy --:-- --



When was this incident detected? \*

mm/dd/yyyy --:-- --



Please enter a brief description of the incident \*

Back

Next

# IMPACT DETAILS 1 OF 7

## Impact Details

Required fields are marked with an asterisk (\*).

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

Additional questions may apply

☐ Yes

☒ No

## System Impact

Please define the functional impact to the organization by selecting one of the following \*

# IMPACT DETAILS 2 OF 7

## System Impact

Please define the functional impact to the organization by selecting one of the following \*

What is the number of systems impacted? \*

How many users are impacted? \*

How was this incident detected?

☐ Administrator

☐ Intrusion Detection System  
(IDS)

☐ User

☐ Unknown

☐ Anti-Virus (AV) Software

☐ Log Review

☐ Other

# IMPACT DETAILS 3 OF 7

What operating systems (OS) are impacted?

Operating System #1



Operating System name

Operating System Version

+ Add Detail For Impacted OS

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)

☐ Mail Server(s)

☐ Router(s)

☐ Switch(es)

☐ Time Server(s)

☐ Web Server(s)

☐ Laptop(s)

☐ Other Server(s)

# IMPACT DETAILS 4 OF 7

Please Enter the Indicator Type

Indicator Type #1

Please Enter the Indicator Type

Indicators

Indicator Context

+ Add Indicator Type

# IMPACT DETAILS 5 OF 7

Enter a Common Vulnerabilities and Exposure Identifier (CVE-ID).

Please do not include the CVE prefix (e.g., 2014-7654321):

## Observed Activity

Where was the activity observed \*

Characterize the observed activity at its most severe level \*



# IMPACT DETAILS 6 OF 7

## Impact Information

What is the known informational impact from the incident? \*

Additional questions may apply

Number of records impacted \*

## Recovery From Incident

Please select the organization's recoverability for this incident \*

Additional questions may apply

# IMPACT DETAILS 7 OF 7

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

☐ Yes

☒ No

[Back](#)

[Review](#)

## 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:** Some entities are regulatory or statutorily required to submit incident reports to DHS, and those entities must provide information in this form as required by applicable statute, regulation, or similar mandate. Failure to provide this information may result in inaccurate record keeping of the entity's compliance. For non-mandatory incident reporting, 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 report.

# 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:** Some entities are regulatorily or statutorily required to submit incident reports to DHS, and those entities must provide information in this form as required by applicable statute, regulation, or similar mandate. Failure to provide this information may result in inaccurate record keeping of the entity's compliance. **For non-mandatory incident reporting, 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 report.**

Version: 3.0 | Report ID: 2021-USCERTv31WBQE8 | Date: 202110121410

Email comments and feedback on the Incident Reporting Form 

# 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 1/31/2028. 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.