

Paperwork Reduction Act

The public reporting burden to complete this information collection is estimated at 10 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and the completing and reviewing the collected information. The collection of information is voluntary. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number and expiration date. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to DHS/CISA/CSD, 245 Murray Lane, SW, Mail Stop 0640, Arlington, VA 20598-0640 ATTN: PRA [OMB Control No. 1670-0037].

Privacy Act Notice

PURPOSE: The Incident Reporting Form enables U.S. Federal Government agencies and external entities to report security incidents, major incidents, breaches, and events 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.

NOTE: Do **not** add sensitive personally identifiable information (SPII) to incident submissions. Any contact information collected will be handled according to the [Department of Homeland Security \(DHS\) privacy policies](#).

DHS Cyber Threat Indicator and Defensive Measure Submission System

<https://www.cisa.gov/forms/share-indicators>

The screenshot shows the homepage of the CISA Cyber Threat Indicator and Defensive Measure Submission System. The browser address bar displays the URL <https://www.cisa.gov/forms/share-indicators>. The page header includes the CISA logo, the text "CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY" and "AMERICA'S CYBER DEFENSE AGENCY", and a search bar. A navigation menu contains links for Topics, Spotlight, Resources & Tools, News & Events, Careers, and About. A prominent red button labeled "REPORT A CYBER ISSUE" is visible. The main heading reads "CISA Cyber Threat Indicator and Defensive Measure Submission System". Below the heading is a horizontal line with a double-headed arrow. At the bottom, a red banner states "CISA Cyber Threat Indicator and Defensive Measure Submission System OMB Control No.: 1670-0037; Expiration Date: 10/31/2024". The footer text begins with "The Cyber Threat Indicator and Defensive Measures Submission System provides a secure, web-enabled method of sharing cyber threat indicators and".

CISA Cyber Threat Indicator and Defensive Measure Submission System OMB Control No.: 1670-0037; Expiration Date: 10/31/2024

The Cyber Threat Indicator and Defensive Measures Submission System provides a secure, web-enabled method of sharing cyber threat indicators and defensive measures with DHS. This system helps analysts to process cyber threat indicators and defensive measures for further sharing with Federal Government and private sector entities. [+ More Detail](#)

Submitter's Contact Information

Please provide your contact information so that we are able to contact you should we need to follow-up.

Name

First *

Last *

Telephone *

Email Address *

Organization Name *

What type of organization are you? *

- United States Federal Government Foreign Government
 Private Sector Individual
 United States State, Local, Tribal, or Territorial (SLTT) Government

Please select the critical infrastructure sector you belong to: *

Organization Country: *

Organization Subdivision: *

Submission Marking Information

Please provide the information below to ensure that your submission is handled appropriately.

Please select the **Traffic Light Protocol (TLP) Color** *

The contact information above, including "Organization Name", may be shared with *

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

Indicators

Indicator Title

Indicator Description

Please enter the Internet Protocol (IP) address observable(s):

IP Address Port Protocol - Remove IP address observable

+ Add another Internet Protocol (IP) address observable

Please enter the Domain observable(s):

Domain - Remove Domain observable

+ Add another Domain observable

Please enter the MD5 Hash observable(s):

MD5 Hash - Remove MD5 hash observable

+ Add another MD5 Hash observable

Please enter the email observable(s):

Email 1

Email Sender

- Remove Email observable 1

Email Sender Spoofed

Email Subject

Email Body

+ Add another Email observable

Please select applicable kill chain stages:

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control
- Action on Objective

Please enter the defensive measures:

Defensive Measure 1

Title

- Remove Defensive Measure 1

Description

+ Add another defensive measure

Additional Defensive Measures

Additional Defensive Measure 1

Title

- Remove Additional Defensive Measure 1

Description

+ Add another additional defensive measure

Attack Patterns

See [Common Attack Patterns Enumeration and Classification \(CAPEC\)](#) for details.

Attack Pattern 1

CAPEC ID

- Remove Attack Pattern 1

CAPEC ID - Remove Attack Pattern 1

Title

Description

+ Add another attack pattern

Vulnerabilities -

See [Common Vulnerabilities and Exposures \(CVE\)](#) for details.

Vulnerability 1

CVE ID - Remove Vulnerability 1

CVE ID - Remove Vulnerability 1

Title

Description

+ Add another vulnerability

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 regarding 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 regarding your request.

CANCEL

NEXT

Version: 1 | Report ID: 2024-INDICATORRYB9U | Date: 202402081351
Please [click here](#) to provide comments and feedback on this form.

[Return to top](#)