

OMB Control Number: 1670-NEW
OMB Expiration Date: MM/DD/YYYY

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/NPPD/CS&C/NCCIC/US-CERT, 245 Murray Lane, SW, Mail Stop 0640, Arlington, VA 20598-0640 ATTN: PRA [OMB Control No. 1670-NEW].

DHS Cyber Threat Indicator and Defensive Measure Submission System

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

The screenshot shows a web browser window with the URL <https://www.us-cert.gov/forms/share-indicators>. The page header includes the US-CERT logo and the text "UNITED STATES COMPUTER EMERGENCY READINESS TEAM". A navigation menu contains links for HOME, ABOUT US, CAREERS, PUBLICATIONS, ALERTS AND TIPS, RELATED RESOURCES, and C' VP. The main content area is titled "DHS Cyber Threat Indicator and Defensive Measure Submission System" and contains a brief description of the system. Below the description is a section titled "Submitter's Contact Information" with a sub-header "Please provide your contact information so that we are able to contact you should we need to follow-up." The form includes input fields for Name (First and Last), Telephone, Email Address, and Organization Name.

DHS Cyber Threat Indicator and Defensive Measure Submission System

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 *

← → <https://www.us-cert.gov/forms/share-indicators> DHS Cyber Threat Indicator... ×

Organization Name *

What type of organization are you? *

United States Federal Government Foreign Government United States State, Local, Tribal, or Territorial (SLTT) Government

Private Sector Individual

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

← → <https://www.us-cert.gov/forms/share-indicators> DHS Cyber Threat Indicator... ×

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):

- Remove Email observable 1
Email Sender

← → <https://www.us-cert.gov/forms/share-indicators> DHS Cyber Threat Indicator... ×

Email 1 × - Remove Email observable 1

Email Sender

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:

← → <https://www.us-cert.gov/forms/share-indicators> DHS Cyber Threat Indicator... ×

Please enter the defensive measures:

Defensive Measure 1 × - Remove Defensive Measure 1

Title

Description

+ Add another defensive measure

Additional Defensive Measures

Additional Defensive Measure 1 × - Remove Additional Defensive Measure 1

Title

Description

+ Add another additional defensive measure

← → <https://www.us-cert.gov/forms/share-indicators> DHS Cyber Threat Indicator... ×

+ Add another additional defensive measure

Attack Patterns

See Common Attack Patterns Enumeration and Classification (CAPEC) for details.

Attack Pattern 1 × - Remove Attack Pattern 1

CAPEC ID

Title

Description

+ Add another attack pattern

Vulnerabilities

See Common Vulnerabilities and Exposures (CVE) for details.

Vulnerability 1 × - Remove Vulnerability 1

← → <https://www.us-cert.gov/forms/share-indicators> DHS Cyber Threat Indicator... ×

Vulnerability 1 × - Remove Vulnerability 1

CVE ID

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.

Version: 1.0 | Report ID: 2017-INDICATOR38J2MB | Date: 201704271202