Review and Confirm Your Submission

Your incident report has NOT yet been submitted. Please review and confirm your submission below.

To submit your report, please review the information below to verify the accuracy of the report and click the SUBMIT button. Or if you would like to revise your incident report you may click the EDIT buttons to return to the previous page.

Contact In	iormati	on
Required fields are marked v	vith an asterisk (*).	
l am: *		
The impacted user	Reporting on	behalf of the impacted user
Your Contact Inform	ation	
First Name	L	_ast Name
first_name		last_name
first name		last_name

11111111111

submitter@email.com

Organization Details

Edit

Required fields are marked with an asterisk (*).

The Impacted Organization's Details

What type of organization are you reporting for?*

Critical Infrastructure and/or Private Sector

Please enter the impacted organization's name or company name (please spell out any acronyms):*

organization_name

Please select the primary Critical Infrastructure sector that the impacted business is involved in:*

Information Technology

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

Incident Description

Edit

Required fields are marked with an asterisk (*).

Incident Description

When approximately, did the incident start? *

11/30/2024, 10:45 AM

When was this incident detected? *

12/02/2024, 10:45 AM

Please enter a brief description of the incident *

Account brute force attempts.

Impact Details

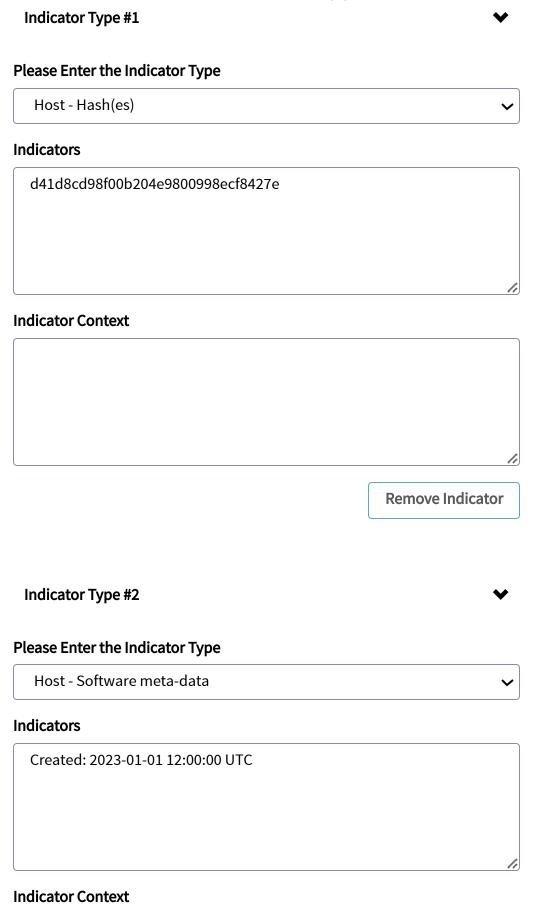
Edit

12/4/24, 10:56 AM

IRF Intake - IRF 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 Denial of Critical Services or Loss of Control What is the number of systems impacted? How many users are impacted? * 100 1 How was this incident detected? Administrator Intrusion Detection System (IDS) Unknown User Anti-Virus (AV) Software Log Review Other

What operating systems (OS) are impacted?

Operating System name	Operating System Version
Windows 10	
	Remove OS
Operating System #2	•
Operating System name	Operating System Version
Linux OS	
	Remove OS
+ Add Detail For Impacted OS	
Application Server(s) Switch(es) Database Server(s) Time Server(s) Desktop(s) Web Server(s) Domain Name Server(s) Laptop(s)	affected? Please select all that apply * Firewall(s) Other Server(s) ICS/SCADA System(s) Mail Server(s) Router(s)
Laptop(s)	



	Remove Indicator
Indicator Type #3	~
ease Enter the Indicator Type	
Host - Software meta-data	~
dicators	
Adobe Reader 11.0.0	
	•
dicator Context	
	Remove Indicator
Indicator Type #4	~
ease Enter the Indicator Type	
case Enter the maleator Type	

dicators	
user@example.com	
licator Context	
	Remove Indicator
	Trainer a marada
ndicator Type #5	•
ndicator Type #5	•
	~
	~
ease Enter the Indicator Type	*
Pase Enter the Indicator Type Network - Network Traffic	*
Network - Network Traffic	•
ase Enter the Indicator Type Network - Network Traffic licators	•
Network - Network Traffic	•
Network - Network Traffic	•
Network - Network Traffic	•
ase Enter the Indicator Type Network - Network Traffic licators TCP/443, UDP/53	
ase Enter the Indicator Type Network - Network Traffic licators TCP/443, UDP/53	
Network - Network Traffic licators TCP/443, UDP/53	
Network - Network Traffic licators TCP/443, UDP/53	
Network - Network Traffic licators TCP/443, UDP/53	
ease Enter the Indicator Type	

lease Enter the Indicator Type	
Host - X.509 Certificate(s)	<u> </u>
dicators	
CN=*.example.com	
	/
dicator Context	
	/
	Remove Indicator
Indicator Type #7	~
lease Enter the Indicator Type	
lease Enter the Indicator Type Network - URL	~
Network - URL	~
Network - URL	~
Network - URL dicators https://malicious.example.com	~
ndicators	

	Remove Indicator
	Nemove marcator
Indicator Type #8	~
ease Enter the Indicator Type	
Network - Email Message(s)	•
dicators	
Email Message(s): Subject: "Important Update"	
dicator Context	
	Remove Indicator
	Remove Indicator
Indicator Type #9	Remove Indicator
Indicator Type #9 lease Enter the Indicator Type	Remove Indicator

ndicators		
\BaseNamedObjects\ExampleMutex		
dicator Context		
		-
	Remove Indicate	or
Indicator Type #10		~
Indicator Type #10		~
		~
		~
lease Enter the Indicator Type Host - User Account(s)		~
lease Enter the Indicator Type Host - User Account(s)		~
lease Enter the Indicator Type Host - User Account(s)		~
ease Enter the Indicator Type Host - User Account(s) dicators		~
Hease Enter the Indicator Type Host - User Account(s) Indicators		~
Hease Enter the Indicator Type Host - User Account(s) Indicators		~
Hease Enter the Indicator Type Host - User Account(s) Idicators Administrator, Guest		~
Hease Enter the Indicator Type Host - User Account(s) Idicators Administrator, Guest		~
Hease Enter the Indicator Type Host - User Account(s) Indicators Administrator, Guest		~
Host - User Account(s) Idicators Administrator, Guest		~
ndicators		~

Indicator Type #11	~
Please Enter the Indicator Type	
Host - System Processes	~
ndicators	
svchost.exe, explorer.exe	
ndicator Context	4
idicator context	
	4
	Remove Indicator
Indicator Type #12	•
Indicator Type #12	•
Please Enter the Indicator Type	
Host - Windows Registry	~
ndicators	
HKEY_LOCAL_MACHINE\Software\Example	

	,
	Remove Indicator
Indicator Type #13	•
lease Enter the Indicator Type	
Network - Domain Name(s)	~
dicators	
evil.example.com	
dicator Context	
	Remove Indicator
Indicator Type #14	•

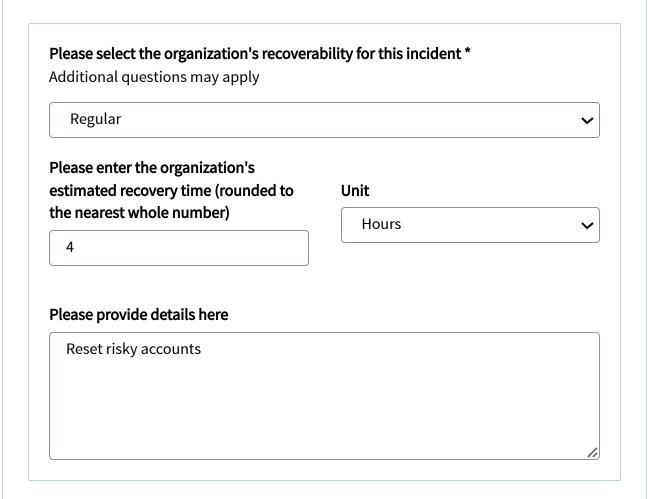
dicators	
AS12345	
dicator Context	/
uicatoi Context	
	Remove Indicator
In diagton Tons o #15	
Indicator Type #15	•
lease Enter the Indicator Type	
Host - File System Directory(ies)	
Those The System Directory (163)	•
ndicators	
C:\Program Files\Example\	
	<i>.</i> /.
ndicator Context	
	Remove Indicator

Planca Enter the Indicator Type	
Please Enter the Indicator Type	
Network - IPv6 Address(es)	~
ndicators	
2001:db8::1234	
ndicator Context	
	,
	Remove Indicator
	Remove mulcator
Indicator Type #17	~
21.	
Please Enter the Indicator Type	
Network - IPv4 Address(es)	~
ndicators	
192.168.1.1	

No Impact



Recovery From Incident



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



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 for 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.

Save and Download Cancel Submit