

Introduction to CISA's Incident Reporting System

March 2022

Introduction to CISA's Incident Reporting System



An Introduction to CISA's Incident Reporting System

Jeremy West CEH[®], CISSP[®], CISM[®], & PMP[®]

Senior Cybersecurity Project Lead
CIAS-ISA

Introduction to CISA's Incident Reporting System

Webinar Agenda

The CISA Incident Reporting System:

- Introduction: CIAS-ISA0
- Overview: CISA'S Incident Reporting System
- Collection, Analysis, Dissemination
- Call to Action
- Questions

Introduction to CISA's Incident Reporting System



This webinar was developed by
the Center for Infrastructure Assurance and Security
at the University of Texas at San Antonio

The CIAS has been working with communities to improve their cybersecurity posture since 2002.

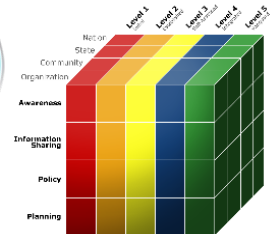
Core competencies include cybersecurity training, exercises, competitions, game development, culture of security initiatives, information sharing and cybersecurity community programs.



Introduction to CISA's Incident Reporting System

About the CIAS-ISAO

- An initiative of the Center for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio
- Focus Areas: Outreach & Grassroots Security
 - Cybersecurity Professional Training & Exercises
 - Cyber Competition Programs
 - Cybersecurity Educational Games
 - Culture of Cybersecurity
 - Information Sharing and Analysis Initiatives
 - National Cybersecurity Preparedness Consortium (NCPC)



Introduction to CISA's Incident Reporting System

Membership Resources

- Educational Content
- Quick Access to National Resources
- Access to Customized Training
- Recorded Webinars
- Discount on Cybersecurity Prep Courses & Workshops
- Roadmap to Establishing an ISAO
- Assessments
- Your CIAS-ISAO Support Team!

Introduction to CISA's Incident Reporting System

Membership Benefits (Levels 2 & 3)

- **Discount on CIAS Prep Courses:** CISSP, CompTIA A+, CompTIA Security+
- Access to **Customized Training** Resources
- Customized **Consultations**
- **Discount on book** "Establishing Cyber Security Programs Through the Community Cyber Security Maturity Model (CCSMM)"
- **Discount on Panoply**, a virtual cyber defense event
- Personalized **Roadmap** to Establishing an ISAO

Introduction to CISA's Incident Reporting System

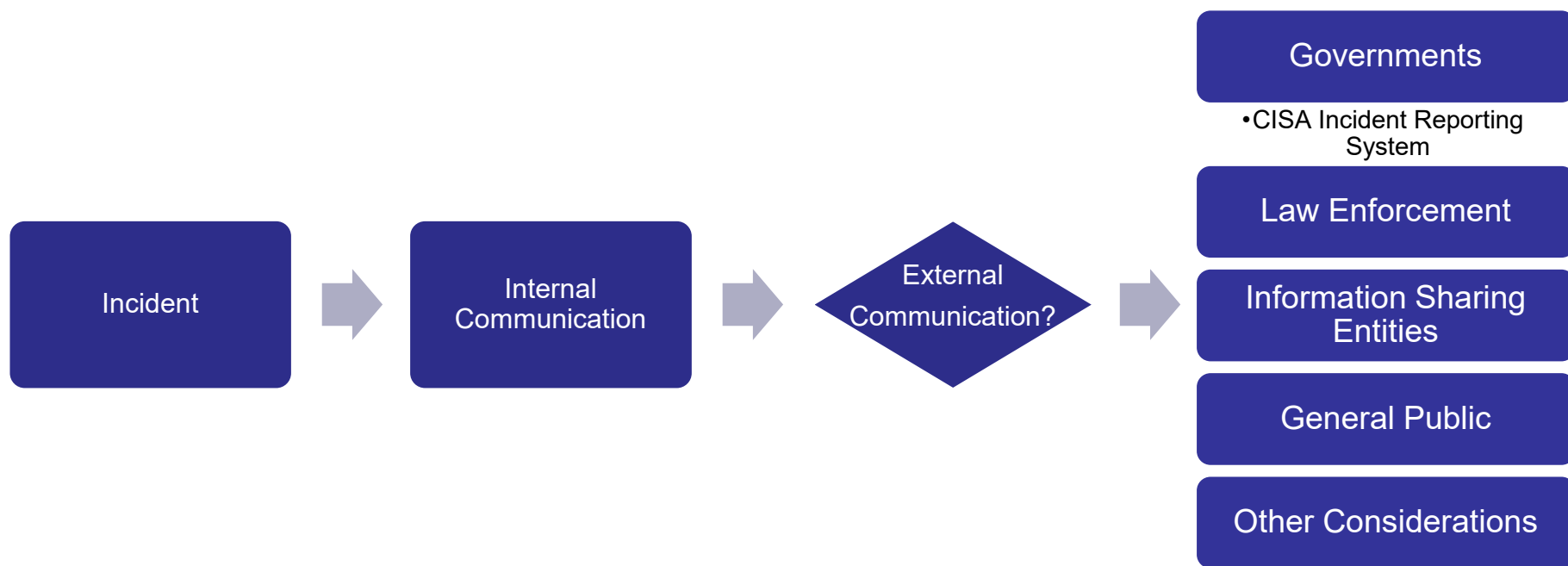
Overview

The CISA Incident Report System assists analysts in providing timely handling of security incidents, improved analysis and potentially assistance with incident response.

- Incident Communication Flow
- Why CISA Incident Reporting System
- Collection, Analysis, Dissemination

Introduction to CISA's Incident Reporting System

Incident Communication Flow



Introduction to CISA's Incident Reporting System

Incident Sharing and Reporting Research

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

Computer Security Incident Handling Guide

ICE Tip Form

If this is an emergency, call 911.

U.S. Immigration and Customs Enforcement

II. Suspected Violation

violation that best applies*

- Marriage Fraud
- Smuggling/Financial Crimes
- Immigration/Pornography
- Other

FEDERAL BUREAU OF INVESTIGATION
INTERNET CRIME COMPLAINT CENTER

Complaint Referral Form
Internet Crime Complaint Center

Note: Fields marked with * are required.

Victim Information

* Name:

* Address:

Address (continued):

Suite/Apt./Mail Stop:

* City:

County:

* Country:

State:

* Zip Code/Route:

* Phone Number:

* Email Address:

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Incident Reporting System OMB Control No.: 1670-0037; Expiration Date: 10/31/2024

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

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

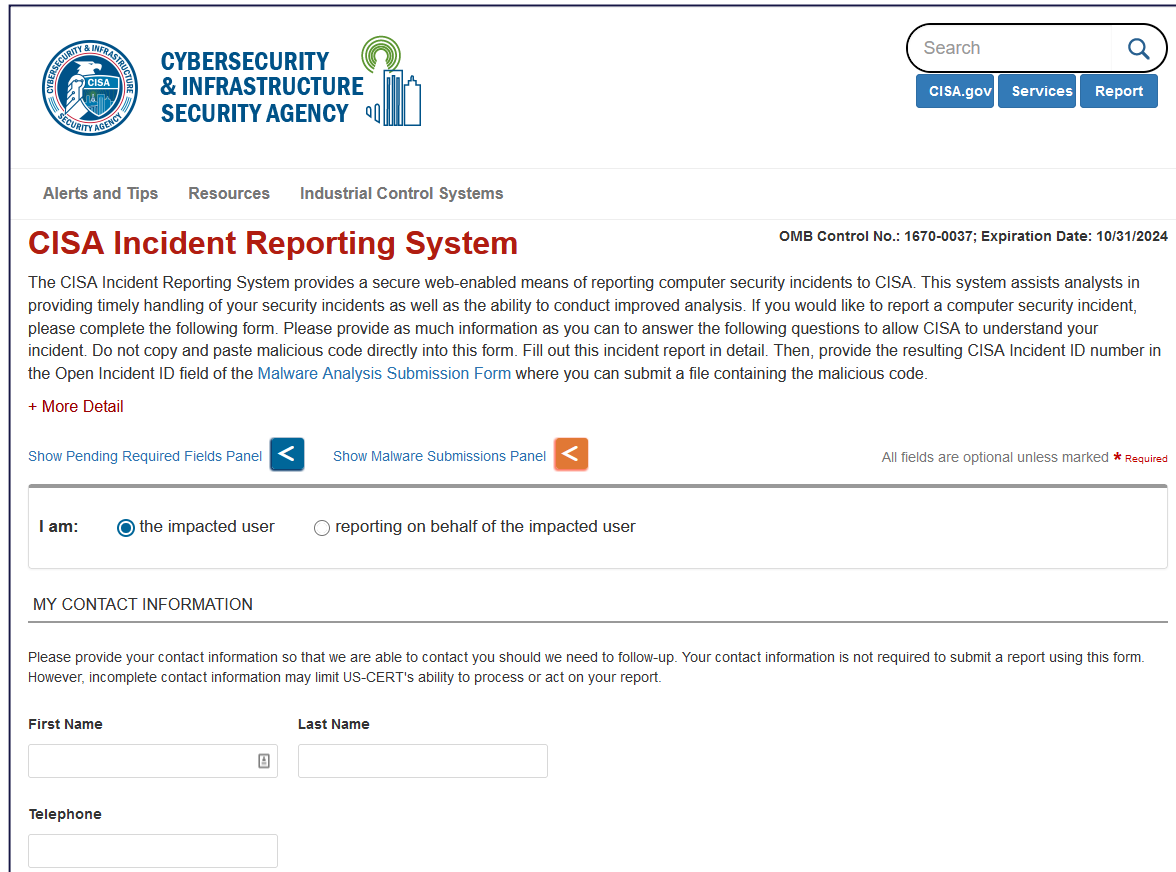
RECOVERY FROM INCIDENT

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

Select One

Introduction to CISA's Incident Reporting System

CISA Incident Reporting System





The screenshot shows the CISA Incident Reporting System web form. 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 buttons for "CISA.gov", "Services", and "Report". Below the header are navigation links for "Alerts and Tips", "Resources", and "Industrial Control Systems". The main heading is "CISA Incident Reporting System" with the OMB Control No.: 1670-0037; Expiration Date: 10/31/2024. The text explains that the system provides a secure web-enabled means of reporting computer security incidents to CISA. It includes a "+ More Detail" link and two expandable panels: "Show Pending Required Fields Panel" and "Show Malware Submissions Panel". A note states "All fields are optional unless marked * Required". The form includes a radio button selection for "I am:" with options "the impacted user" (selected) and "reporting on behalf of the impacted user". Below this is the "MY CONTACT INFORMATION" section, which includes a paragraph explaining that contact information is required for follow-up. The form fields include "First Name", "Last Name", and "Telephone".

CISA Incident Reporting System OMB Control No.: 1670-0037; Expiration Date: 10/31/2024

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. 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.

[+ More Detail](#)

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

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

<https://us-cert.cisa.gov/forms/report>

Introduction to CISA's Incident Reporting System

Caveats

- Provide as much information as you can to allow CISA to understand your incident.
- This website uses SSL /TLS to provide more secure communications than unencrypted email.
- Do not copy and paste malicious code directly into this form.
- Refrain from including PII or SPII in incident submissions unless necessary.
- Understand the Privacy Act Statement at the bottom of the page
- 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.
- 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.

Introduction to CISA's Incident Reporting System

Collection



COLLECTION



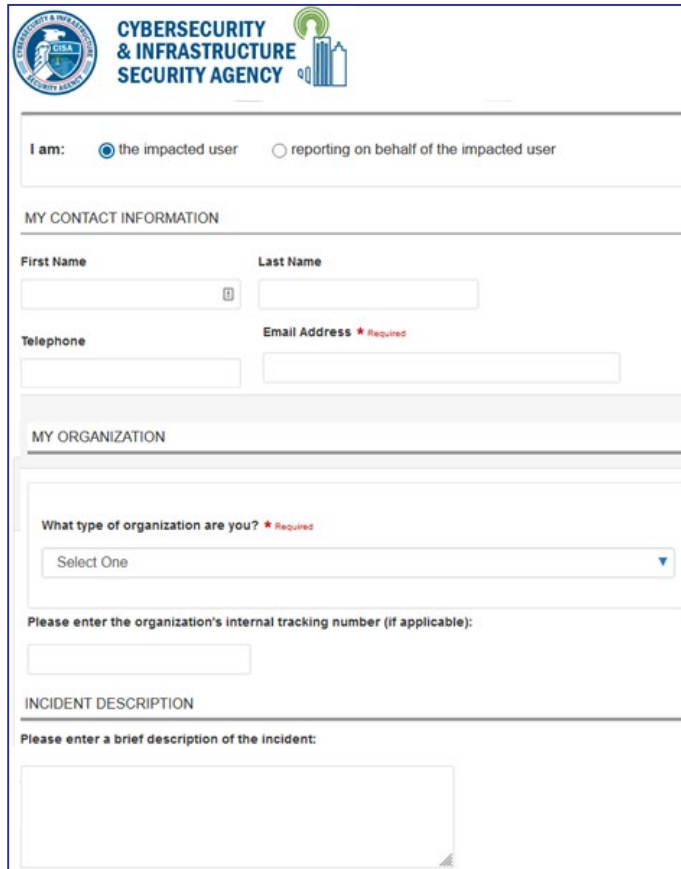
ANALYSIS



DISSEMINATION

Introduction to CISA's Incident Reporting System

Collection: Cyber Incident



The screenshot shows the CISA Incident Reporting System form for a Cyber Incident collection. The form is titled "CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY" and includes the following sections:

- I am:** the impacted user reporting on behalf of the impacted user
- MY CONTACT INFORMATION**
 - First Name:
 - Last Name:
 - Telephone:
 - Email Address * Required:
- MY ORGANIZATION**
 - What type of organization are you? * Required:
 - Please enter the organization's internal tracking number (if applicable):
- INCIDENT DESCRIPTION**
 - Please enter a brief description of the incident:

Contact information

- Name
- Phone Number
- Email Address
- Tracking number

Date and Time

- Incident start
- Incident discovery

Brief description of incident

Introduction to CISA's Incident Reporting System

Analysis



COLLECTION



ANALYSIS



DISSEMINATION

Introduction to CISA's Incident Reporting System

Analysis

At a basic level we can perform elementary analysis on a cyber incident by answering the following questions:

- Was confidentiality, integrity, or availability potentially compromised?
- What types of information did technical staff discover regarding the incident?
- What is the functional and information impact?
- What is the organization's ability to recover from the incident?

Introduction to CISA's Incident Reporting System

Analysis: CIA

IMPACT DETAILS
Was the confidentiality, integrity, and/or availability of your organization's information systems potentially compromised? * Required
<input type="radio"/> Yes <input type="radio"/> No

When determining if confidentiality, integrity or availability have been impacted, consider the following questions:

- **Confidentiality:** Was there potential or actual unauthorized access to protected or sensitive information?
- **Integrity:** Was there an unauthorized or unintended modification of information or systems?
- **Availability:** Did authorized users have timely and uninterrupted access to information and systems?

Introduction to CISA's Incident Reporting System

Analysis

- Technical Details
- Impact
 - Functional
 - Information
- Recovery



Introduction to CISA's Incident Reporting System

Analysis: Technical



[This Photo](#) by Unknown Author is licensed under [CC BY-NC-ND](#)

Additional technical analysis may reveal:

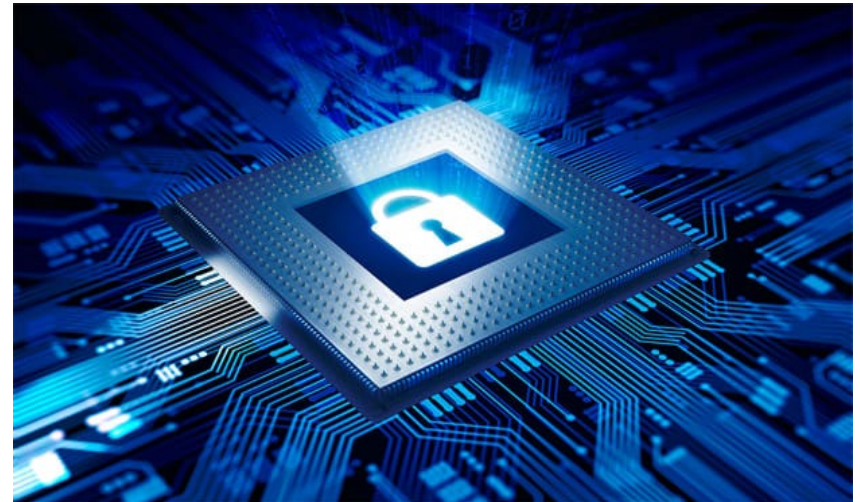
- System/Incident Info
 - IP Addresses
 - OS
 - System Functions
 - CVE
- Observed Activities

Introduction to CISA's Incident Reporting System

Analysis: Impact

There are two types of impact worthy of measurement and quantification:

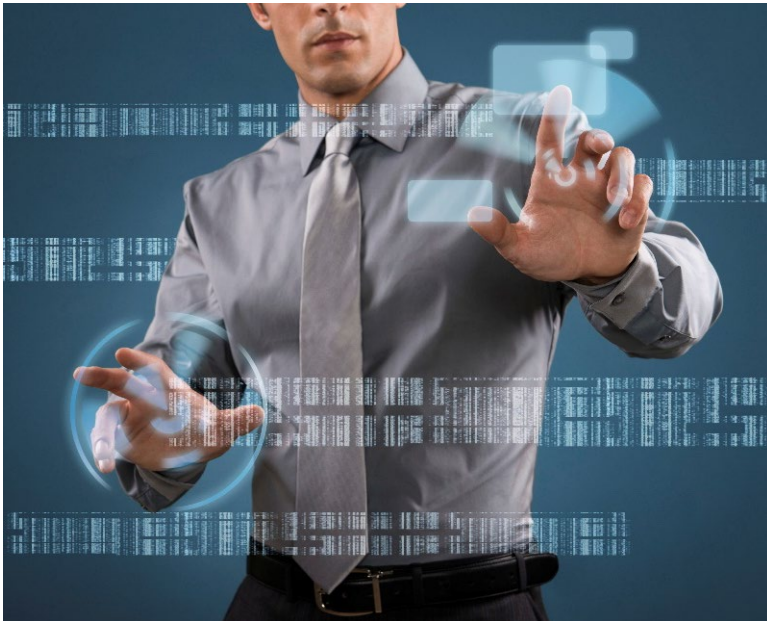
- **Functional Impact**
 - Impact to business functionality or ability to provide services
- **Information Impact**
 - Describes the type of information:
 - Lost
 - compromised
 - corrupted



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

Introduction to CISA's Incident Reporting System

Analysis: Functional Impact



[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)

No Impact

Impact to Non-Critical Services

Impact to Critical Services

Denial of Non-Critical Services

Denial of Critical Services or Loss of Control

Introduction to CISA's Incident Reporting System

Analysis: Information Impact

Suspected

Privacy Data Breach

Proprietary Data Breach

Destruction of Non-Critical System

Critical System Data Breach

Core Credential Compromise

Destruction of Critical System



[This Photo](#) by Unknown Author is licensed under [CC BY](#)

Introduction to CISA's Incident Reporting System

Analysis: Recoverability

Recoverability identifies the scope of resources needed to get back to baseline after an incident.



[This Photo](#) by Unknown Author is licensed under [CC BY](#)

Regular

Supplemented

Extended

Not Recoverable

Introduction to CISA's Incident Reporting System

Upload the Malware



CISA Incident Reporting System OMB Control No.: 1670-0037; Expiration Date: 10/31/2024

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

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*

RECOVERY FROM INCIDENT

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

Select One

Cancel

Next



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

US-CERT AMAC Malware Analysis Submissions

(All fields are optional)

Agree to Terms:

First Name:

Last Name:

Organization:

Incident ID:

Phone Number:

Email Address:

Please enter context regarding this submission:

Select file (100MB Limit):

Submit

Browse... No file selected.

Introduction to CISA's Incident Reporting System

Dissemination



COLLECTION



ANALYSIS



DISSEMINATION

Introduction to CISA's Incident Reporting System

Dissemination

The purpose of dissemination is to ensure information is distributed so that entities can make decisions and/or act to reduce risk.



Introduction to CISA's Incident Reporting System

Dissemination: Information Sharing Report



Collect: Contact information and incident details



Analyze: Impact and recoverability



Disseminate: Determine audience and distribute

Introduction to CISA's Incident Reporting System

Basic Information Sharing Report

Modeled after CISA's Incident Reporting System because:

- Encourages reporting to a centralized body
- Maps to other reporting systems
- Simplified approach



Introduction to CISA's Incident Reporting System

Information Sharing Report Highlights

- Contact information
- Target audience
- Incident details
- Impact
- Recoverability



Introduction to CISA's Incident Reporting System

Call to Action

- **Take our course:** MGT-473 Organizational Information Sharing
- **Review CISA's Incident Reporting System** and determine when it's appropriate for your organization to escalate/report to CISA.
- **Review your organization's** internal and external incident collection, analysis, and dissemination practices to ensure you are collecting everything CISA needs in the reporting system.
- **Download** the CIAS Information Sharing Template form from your CIAS-ISA membership portal.

Introduction to CISA's Incident Reporting System

Thank you!

In addition to today's webinar, we can help you with:

- Training & Exercises
- Implementing a Culture of Cybersecurity & K-12 Educational Cybersecurity Program
- Customized Cybersecurity Competitions
- Assessments
- Access to Educational Content
- ISAO Support for Communities
- Establishing and Growing a Program (CCSMM)

Introduction to CISA's Incident Reporting System

Questions?

Jeremy West
Senior Cybersecurity Project Lead
Jeremy.West@utsa.edu

Julina Macy
Director of Communications
Julina.Macy@utsa.edu

CIASISAO.org