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-ISAO

Webinar Agenda

The CISA Incident Reporting System:

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

Introduction to CISA's Incident Reporting System

CIAS-ISA
COMMUNITY CYBERSECURITY PROGRAMS

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

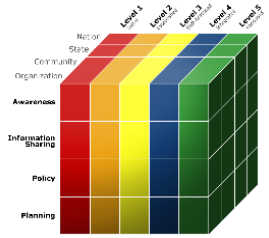
The CIAS has been working with communities to improve their cybersecurity posture since 2002.

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

UTSA

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)



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!

Membership Benefits (Levels 2 & 3)

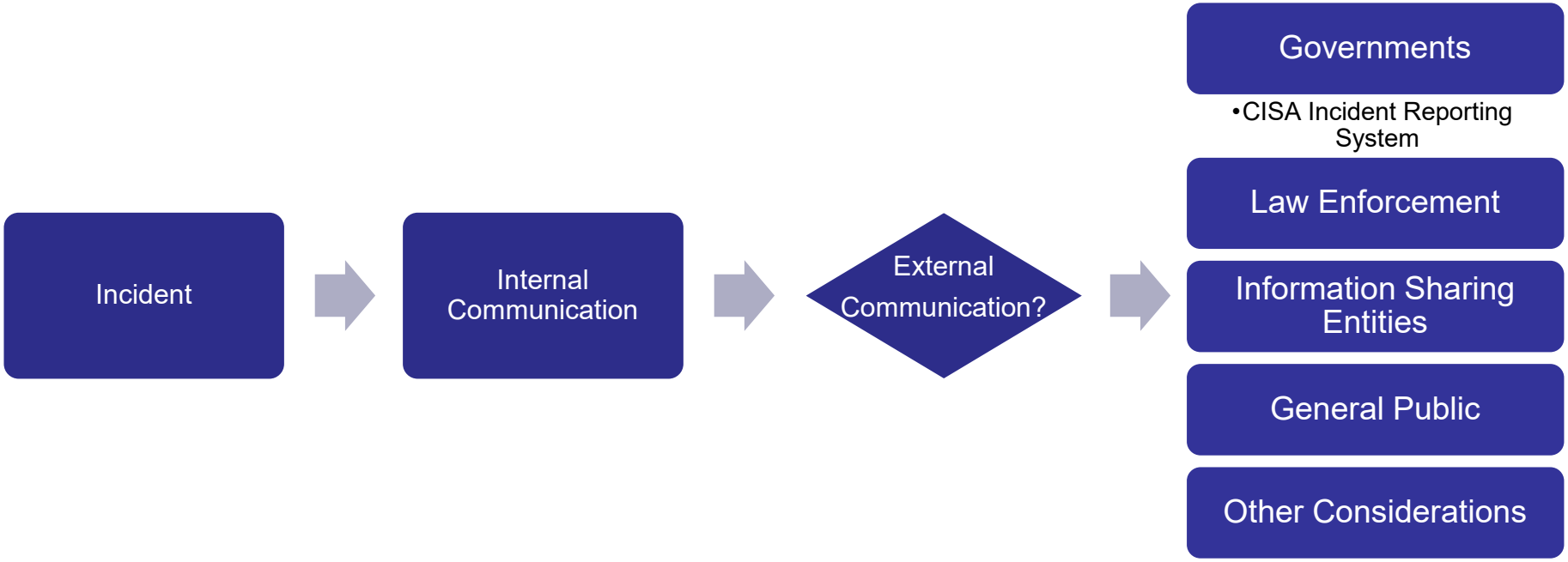
- **Discount on CIAS Prep Courses**: CISSP, CompTIA A+, CompTIA Security+
- Access to **Customized Training** Resources
- Customized **Consultations**
- **Discount on book** "Establishing Cyber Security Programs Through the Community Cyber Security Maturity Model (CCSMM)"
- **Discount on Panoply**, a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

Overview

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

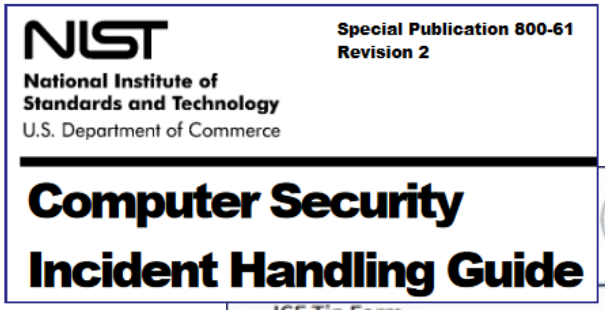
- Incident Communication Flow
- Why CISA Incident Reporting System
- Collection, Analysis, Dissemination

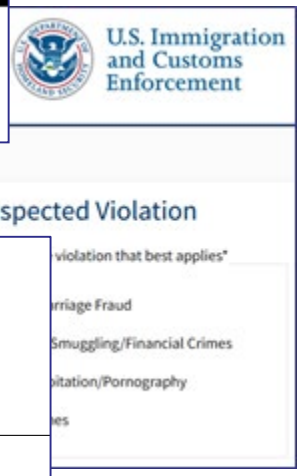
Incident Communication Flow

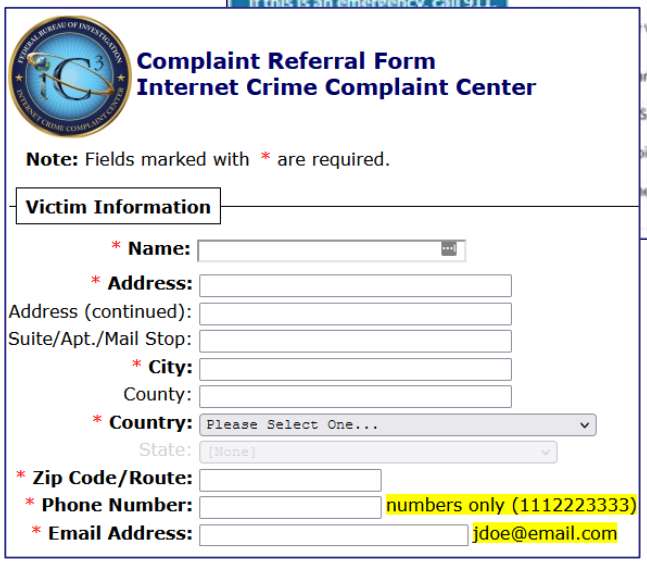


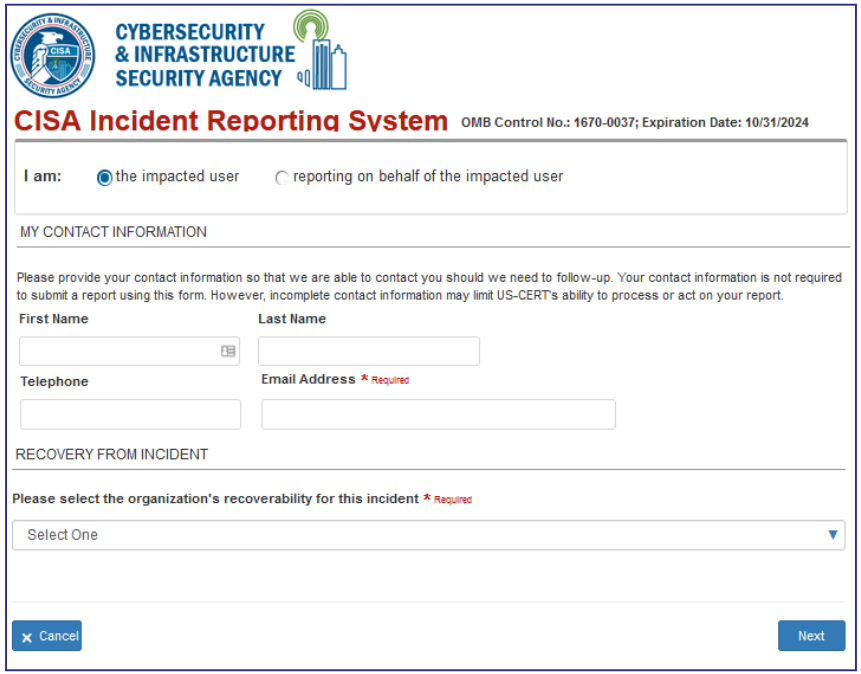
Introduction to CISA's Incident Reporting System

Incident Sharing and Reporting Research

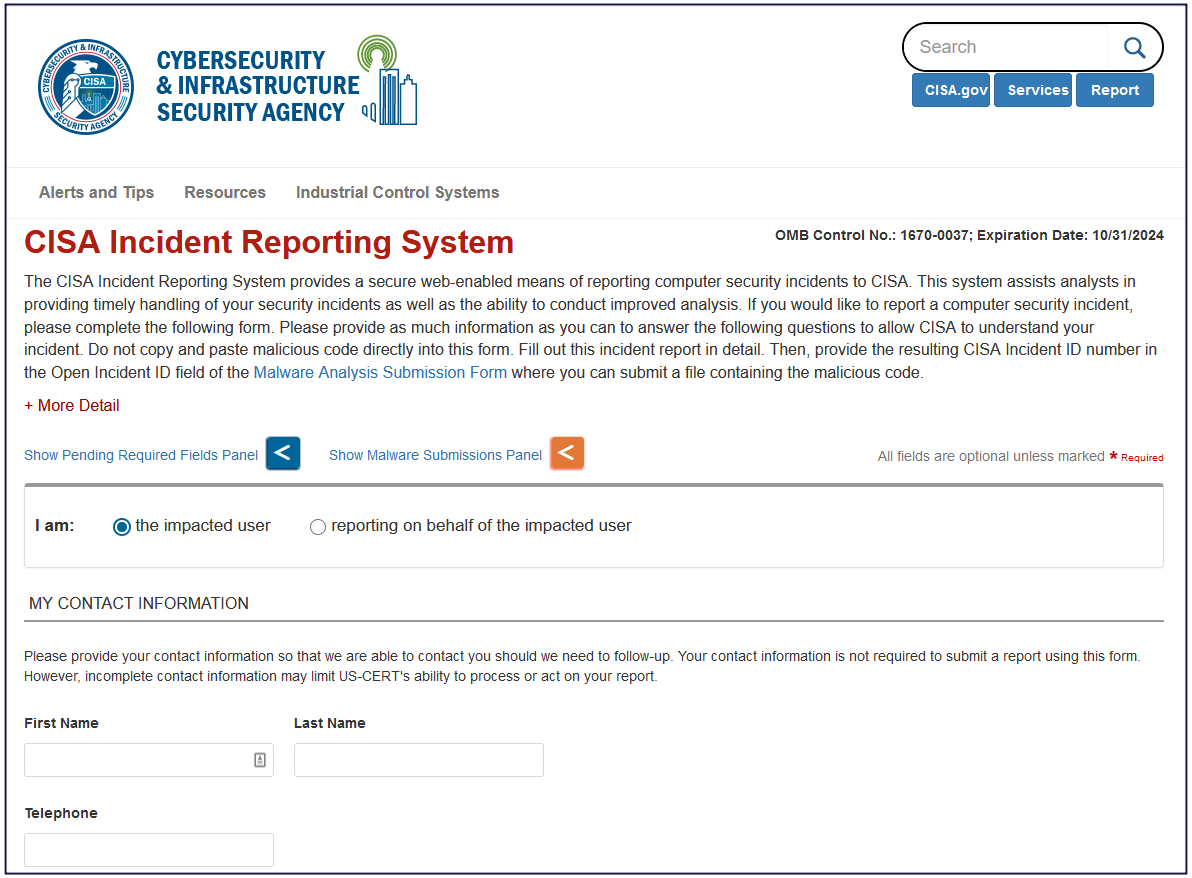








CISA Incident Reporting System



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

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.

Collection

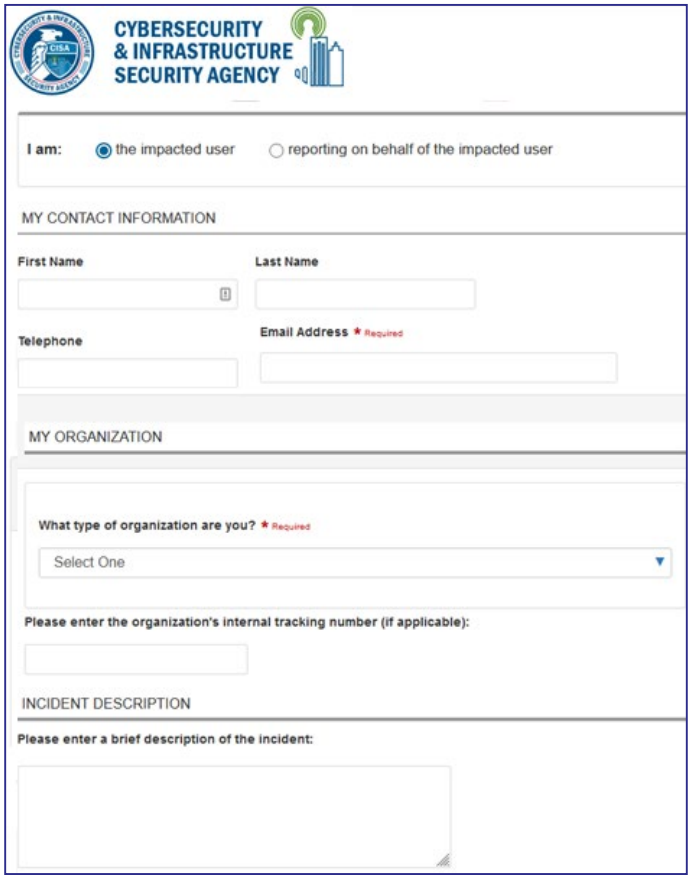
COLLECTION

ANALYSIS

DISSEMINATION

Introduction to CISA's Incident Reporting System

Collection: Cyber Incident



Contact information

- Name
- Phone Number
- Email Address
- Tracking number

Date and Time

- Incident start
- Incident discovery

Brief description of incident

Analysis

COLLECTION

ANALYSIS

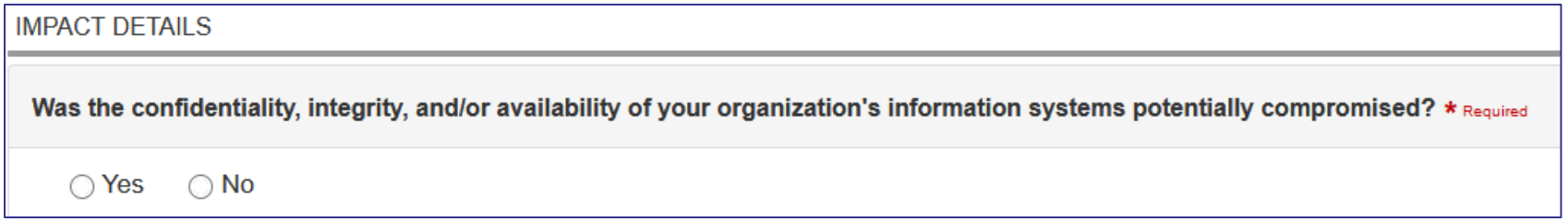
DISSEMINATION

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?

Analysis: CIA

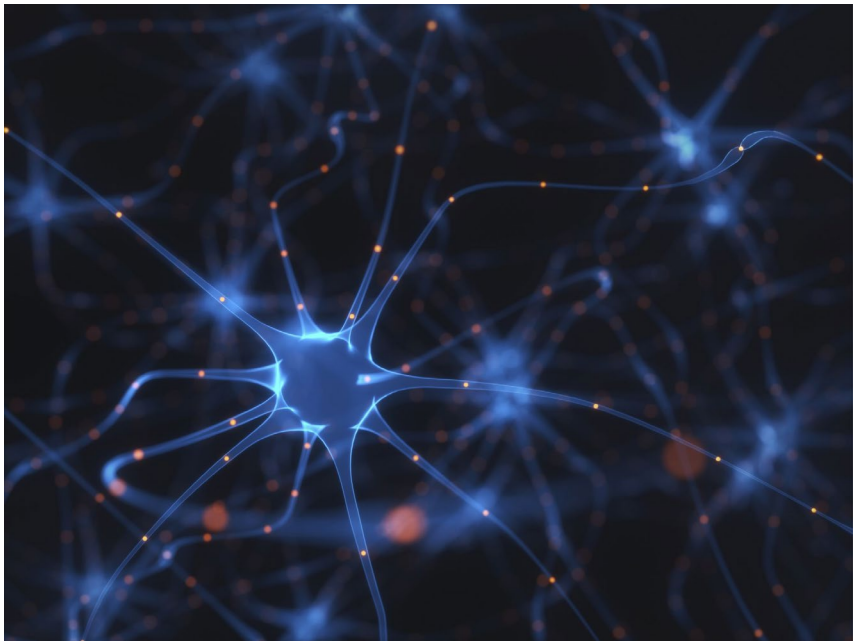


When determining if confidentiality, integrity or availability have been impacted, consider the following questions:

- **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?

Analysis

- Technical Details
- Impact
  - Functional
  - Information
- Recovery



Analysis: Technical

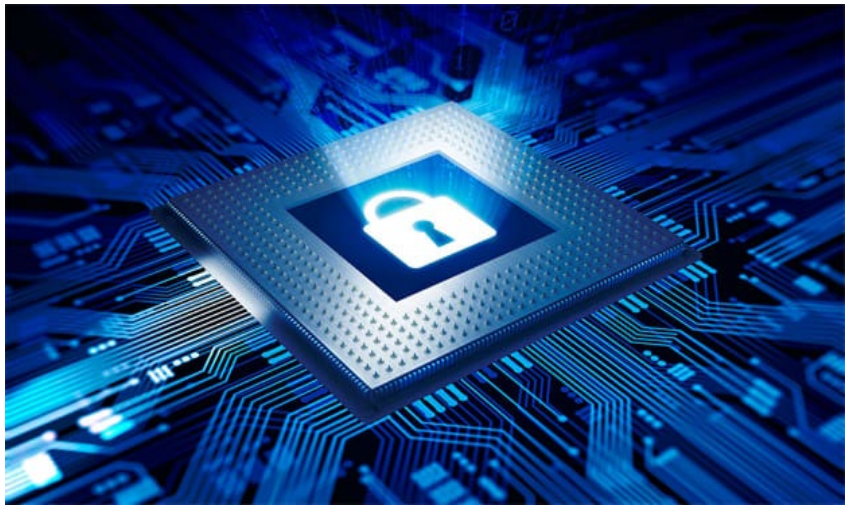
Additional technical analysis may reveal:

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

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



Analysis: Functional Impact

- No Impact
- Impact to Non-Critical Services
- Impact to Critical Services
- Denial of Non-Critical Services
- Denial of Critical Services or Loss of Control

Analysis: Information Impact

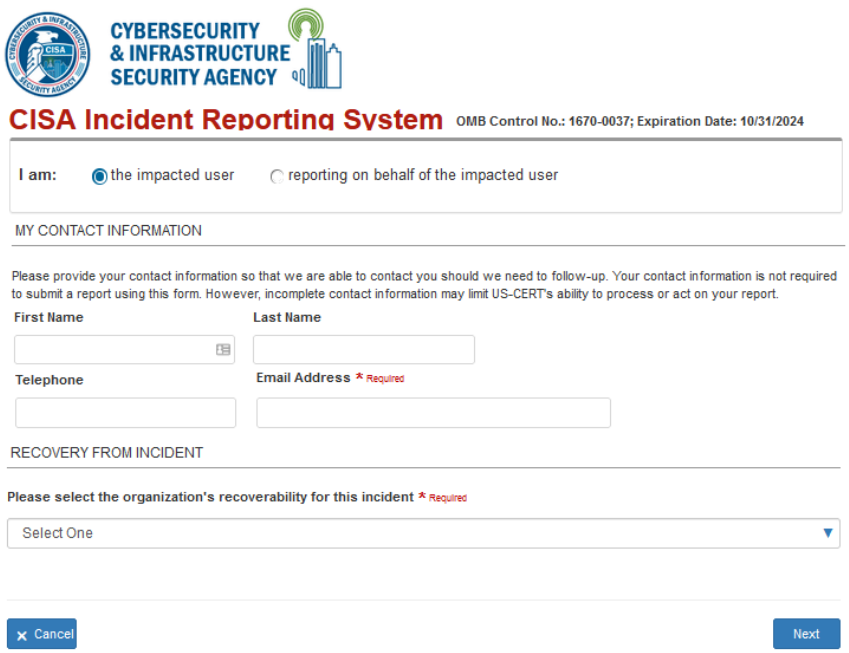
- Suspected
- Privacy Data Breach
- Proprietary Data Breach
- Destruction of Non-Critical System
- Critical System Data Breach
- Core Credential Compromise
- Destruction of Critical System

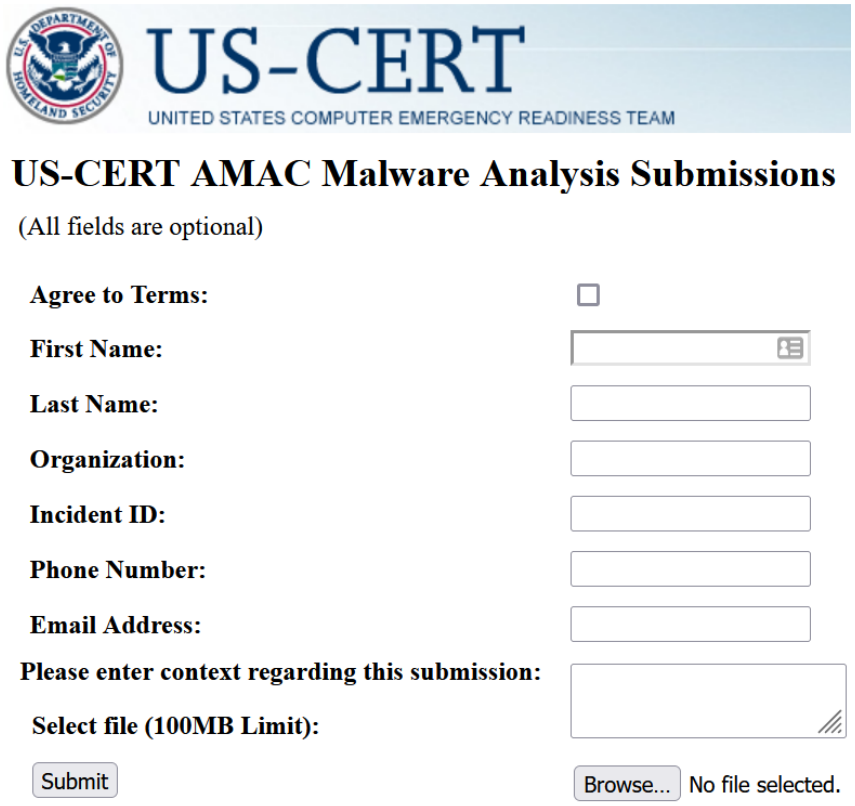
Analysis: Recoverability

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

- Regular
- Supplemented
- Extended
- Not Recoverable

Upload the Malware





Dissemination

COLLECTION

ANALYSIS

DISSEMINATION

Dissemination

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

Dissemination: Information Sharing Report

Collect: Contact information and incident details

Analyze: Impact and recoverability

Disseminate: Determine audience and distribute

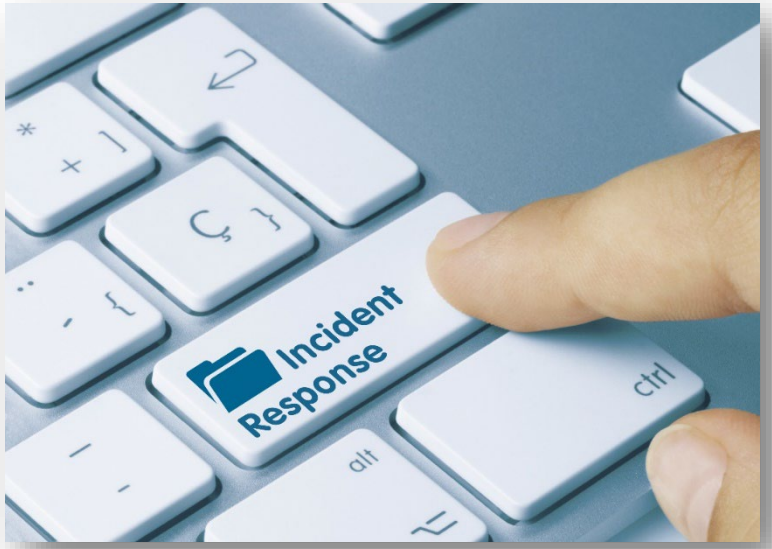
Basic Information Sharing Report

Modeled after CISA's Incident Reporting System because:

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

Information Sharing Report Highlights

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



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-ISAO membership portal.

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