FRSecure CISSP Mentor Program

2022

Class #10 – Domain 7

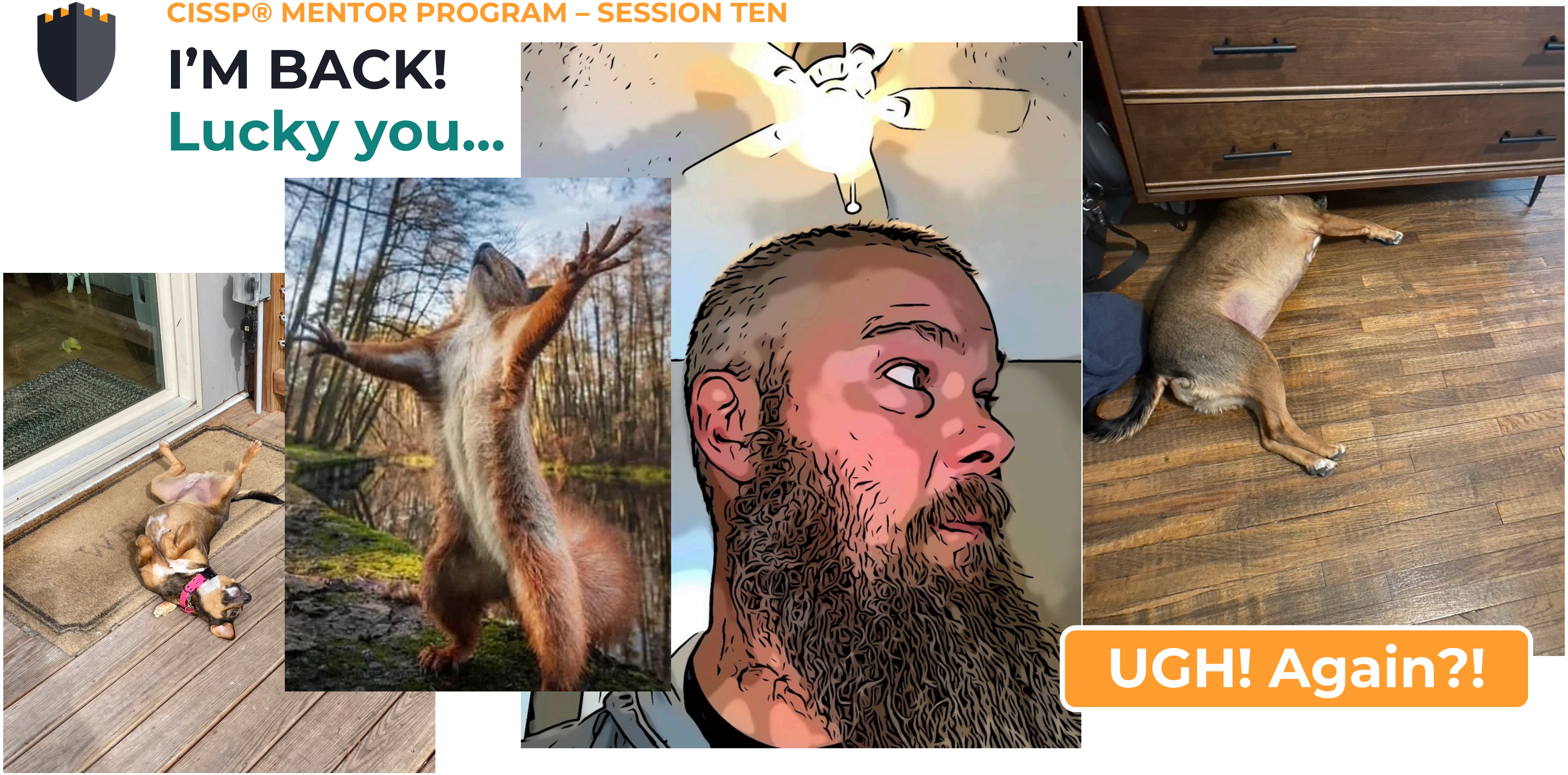
Evan Francen

Evan Francen – FRSecure and SecurityStudio Co-Founder & CEO

CISSP® MENTOR PROGRAM – SESSION TEN

I'M BACK!

Lucky you…



CISSP® MENTOR PROGRAM – SESSION TEN

INTRODUCTION

Agenda

- Welcome, Reminders, & Introduction
- Questions
- **Domain 7 – Communication and Network Security (pp. 463 - Kindle)**

CISSP® MENTOR PROGRAM – SESSION TEN

INTRODUCTION

Agenda

- Welcome, Reminders, & Introduction
- Questions
- **Domain 7 – Communication and Network Security (pp. 463 - Kindle)**

Only 15 sections to cover in this most excellent domain…

CISSP® MENTOR PROGRAM – SESSION TEN

FRSECURE CISSP MENTOR PROGRAM LIVE STREAM

THANK YOU!

Quick housekeeping reminder.

- The online/live chat that's provided while live streaming on YouTube is for constructive, respectful, and relevant (about course content) discussion **ONLY**.
- At **NO TIME** is the online chat permitted to be used for disrespectful, offensive, obscene, indecent, or profane remarks or content.
- Please do not comment about controversial subjects, and please **NO DISCUSSION OF POLITICS OR RELIGION**.
- Failure to abide by the rules may result in disabling chat for you.
- **DO NOT** share or post copywritten materials. (pdf of book)

GETTING GOING…

Managing Risk!

Study Tips:

- Study in small amounts frequently (20-30 min)
- Flash card and practice test apps help
- Take naps after heavy topics (aka Security Models)
- Write things down, say them out loud
- Use the Slack Channels
- Exercise or get fresh air in between study sessions

GETTING GOING…

Managing Risk!

Study Tips:

- Study in small amounts frequently (20-30 min)
- Flash card and practice test apps help
- Take naps after heavy topics (aka Security Models)
- Write things down, say them out loud
- Use the Slack Channels
- Exercise or get fresh air in between study sessions

Stick with it. You'll be glad you did. I promise.

GETTING GOING…
THANK YOU!

- **Christophe** – GREAT job Monday on Domain #6 - Security Assessment and Testing!
- **Ryan** is keeping us ready with all the live streamy techy stuff!
- **Ron** is still EL MEJOR PROFESOR! Answering questions ALL DAY.
- **Brandon Matis** running things and things.
- Many unsung **FRSecure heroes** doing heroey things.

CISSP® MENTOR PROGRAM – SESSION TEN

GETTING GOING...

T

CISSP® MENTOR PROGRAM – SESSION TEN

INTRODUCTION

Agenda

- ~~Welcome, Reminders, & Introduction~~
- Questions
- **Domain 7 – Security Operations (pp. 463 - Kindle)**

CISSP® MENTOR PROGRAM – SESSION TEN

QUESTIONS.

10

How about some practice ones?

1. What is the essential difference between a self-audit and an independent audit?
   a. Tools used
   b. Competence
   c. Results
   d. Objectivity

QUESTIONS.

How about some practice ones?

1. What is the essential difference between a self-audit and an independent audit?
   a. Tools used
   b. Competence
   c. Results
   d. **Objectivity**

QUESTIONS.

10

How about some practice ones?

2. **Which of the following is the process of repeating a portion of a test scenario or test plan to ensure that changes in information system have not introduced any errors?**

   a. Black box testing

   b. Pilot Testing

   c. Parallel Test

   d. Regression Testing

CISSP® MENTOR PROGRAM – SESSION TEN

QUESTIONS.

How about some practice ones?

2. **Which of the following is the process of repeating a portion of a test scenario or test plan to ensure that changes in information system have not introduced any errors?**

   a. Black box testing

   b. Pilot Testing

   c. Parallel Test

   d. **<u>Regression Testing</u>**

CISSP® MENTOR PROGRAM – SESSION TEN

QUESTIONS.

10

How about some practice ones?

3. **What would a significant benefit be from conducting an unannounced penetration test?**

   a. The pen test would be a more realistic analysis of the target network

   b. The security analyst could not provide an honest analysis

   c. It is best to catch critical infrastructure unpatched:

   d. Network security would be in a "best state" posture

QUESTIONS.

How about some practice ones?

3. What would a significant benefit be from conducting an unannounced penetration test?

   a. The pen test would be a more realistic analysis of the target network

   b. The security analyst could not provide an honest analysis

   c. It is best to catch critical infrastructure unpatched

   d. Network security would be in a "best state" posture

CISSP® MENTOR PROGRAM – SESSION TEN

QUESTIONS.

10

How about some practice ones?

4. **Which of the following answers represents part of the attack phase of a penetration test?**
   a. Getting the legal documents signed
   b. Active or Passive Reconnaissance
   c. Escalate Privileges
   d. Removing all tools and exploits:

QUESTIONS.

How about some practice ones?

4. **Which of the following answers represents part of the attack phase of a penetration test?**

   a. Getting the legal documents signed

   b. Active or Passive Reconnaissance

   c. **Escalate Privileges**

   d. Removing all tools and exploits:

CISSP® MENTOR PROGRAM – SESSION TEN

QUESTIONS.

10

How about some practice ones?

5. **Which well-known model is used for understanding the maturity level of a process?**
   a. The Zachman Framework
   b. CMM - Capability Maturity Model
   c. HIPAA
   d. PCI-DSS

QUESTIONS.

How about some practice ones?

5. **Which well-known model is used for understanding the maturity level of a process?**

   a. The Zachman Framework

   b. CMM - Capability Maturity Model

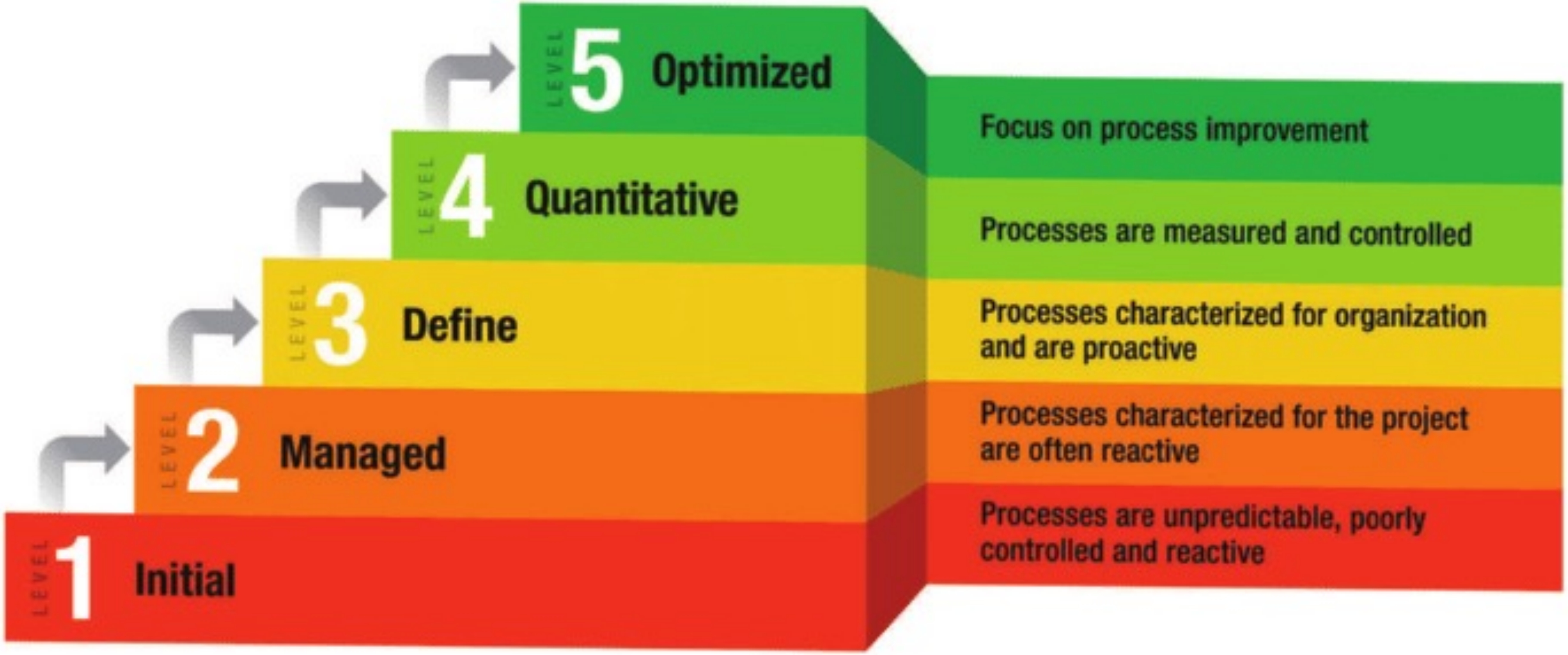
   c. HIPAA

   d. PCI-DSS

CISSP® MENTOR PROGRAM – SESSION TEN

QUESTIONS.

!



LEVEL 5 Optimized: Focus on process improvement

LEVEL 4 Quantitative: Processes are measured and controlled

LEVEL 3 Define: Processes characterized for organization and are proactive

LEVEL 2 Managed: Processes characterized for the project are often reactive

LEVEL 1 Initial: Processes are unpredictable, poorly controlled and reactive

?

CISSP® MENTOR PROGRAM – SESSION TEN

QUESTIONS.

10

How about some practice ones?

6. **What would you call a collection of tools that allow enterprises to continually and consistently simulate the full attack cycle (including insider threats, lateral movement, and data exfiltration) against enterprise infrastructure, using software agents, virtual machines, and other means?**

   a. The pandora toolbox

   b. Advanced Persistent Threats

   c. Such a collection of tools does not exist

   d. Breach & attack Simulation

QUESTIONS.

How about some practice ones?

6. **What would you call a collection of tools that allow enterprises to continually and consistently simulate the full attack cycle (including insider threats, lateral movement, and data exfiltration) against enterprise infrastructure, using software agents, virtual machines, and other means?**

a. The pandora toolbox

b. Advanced Persistent Threats

c. Such a collection of tools does not exist

d. Breach & attack Simulation

CISSP® MENTOR PROGRAM – SESSION TEN

QUESTIONS.

10

How about some practice ones?

7. **Organizations should not view disaster recovery as which of the following?**
   a. Committed expense
   b. Enforcement of legal statutes
   c. Compliance with regulations
   d. Discretionary expense

CISSP® MENTOR PROGRAM – SESSION TEN

QUESTIONS.

How about some practice ones?

7. **Organizations should not view disaster recovery as which of the following?**

   a. Committed expense

   b. Enforcement of legal statutes

   c. Compliance with regulations

   d. **Discretionary expense**

QUESTIONS.

10

How about some practice ones?

8. What is a common way of preventing users from running code that has been altered or corrupted since it was originally approved and installed?

   a. Software Accreditation

   b. IDEA - International Data Encryption Algorithm

   c. Code Signing

   d. Code Hashing

QUESTIONS.

How about some practice ones?

8. What is a common way of preventing users from running code that has been altered or corrupted since it was originally approved and installed?

   a. Software Accreditation

   b. IDEA - International Data Encryption Algorithm

   c. **Code Signing**

   d. Code Hashing

CISSP® MENTOR PROGRAM – SESSION TEN

QUESTIONS.

10

How about some practice ones?

9. **Which answer is generally not associated with a resource exhaustion attack?**
   a. Teardrop Attack
   b. Fork Bomb
   c. Smurf Attack
   d. Memory Leak

CISSP® MENTOR PROGRAM – SESSION TEN

QUESTIONS.

How about some practice ones?

9. **Which answer is generally not associated with a resource exhaustion attack?**

   a. Teardrop Attack

   b. Fork Bomb

   c. Smurf Attack

   d. Memory Leak

CISSP® MENTOR PROGRAM – SESSION TEN

QUESTIONS.

10

How about some practice ones?

10. What process can tell an executive manager about the state of the organization's security program?

   a. Internal Risk Assessment

   b. A Security Audit

   c. Change Control Processes

   d. Security Incident Logs

CISSP® MENTOR PROGRAM – SESSION TEN

QUESTIONS.

How about some practice ones?

10. **What process can tell an executive manager about the state of the organization's security program?**

    a. Internal Risk Assessment

    b. A Security Audit

    c. Change Control Processes

    d. Security Incident Logs

QUESTIONS.

How about some practice ones?

10. What process can tell an executive manager about the state of the organization's security program?

    a. Internal Risk Assessment

    b. A Security Audit

    c. Change Control Processes

    d. Security Incident Logs

There!

10 outta 10.

CISSP® MENTOR PROGRAM – SESSION TEN

INTRODUCTION

Agenda

- ~~Welcome, Reminders, & Introduction~~
- ~~Questions~~
- **Domain 7 – Security Operations (pp. 463 - Kindle)**

CISSP® MENTOR PROGRAM – SESSION TEN

INTRODUCTION

Agenda

- ~~Welcome, Reminders, & Introduction~~
- ~~Questions~~
- **Domain 7 – Security Operations (pp. 463 - Kindle)**

Now this…

CISSP® MENTOR PROGRAM – SESSION TEN

INTRODUCTION

Agenda

Domain 7 – Security Operations (pp. 463 - Kindle)

- 7.1 - Understand and comply with investigations
- 7.2 - Conduct logging and monitoring activities
- 7.3 - Perform Configuration Management (CM) (e.g., provisioning, baselining, automation)
- 7.4 - Apply foundational security operations concepts
- 7.5 - Apply resource protection
- 7.6 - Conduct incident management
- 7.7 - Operate and maintain detective and preventative measures
- 7.8 - Implement and support patch and vulnerability management

CISSP® MENTOR PROGRAM – SESSION TEN

INTRODUCTION

Agenda

Domain 7 – Security Operations (pp. 463 - Kindle)

- 7.9 - Understand and participate in change management processes
- 7.10 - Implement recovery strategies
- 7.11 - Implement Disaster Recovery (DR) processes
- 7.12 - Test Disaster Recovery Plans (DRP)
- 7.13 - Participate in Business Continuity (BC) planning and exercises
- 7.14 - Implement and manage physical security
- 7.15 - Address personnel safety and security concern

CISSP® MENTOR PROGRAM – SESSION TEN

INTRODUCTION

Agenda

Domain 7 – Security Operations (pp. 463 - Kindle)

- 7.9 - Understand and participate in change management processes
- 7.10 - Implement recovery strategies
- 7.11 - Implement Disaster Recovery (DR) processes
- 7.12 - Test Disaster Recovery Plans (DRP)
- 7.13 - Participate in Business Continuity (BC) planning and exercises
- 7.14 - Implement and manage physical security
- 7.15 - Address personnel safety and security concern

Alright, piece of cake.

CISSP® MENTOR PROGRAM – SESSION TEN

INTRODUCTION

Agenda

Domain 7 – Security Operations (pp. 463 - Kindle)

- 7.9 - Und sses
- 7.10 - Im
- 7.11 - Imp
- 7.12 - Tes
- 7.13 - Participate in Business Continuity (BC) planning and exercises
- 7.14 - Implement and manage physical security
- 7.15 - Address personnel safety and security concern

Hold up a second though…

Alright, piece of cake.

CISSP® MENTOR PROGRAM – SESSION TEN

DAD JOKE…

If you don’t like it, it’s Brad’s fault!

CISSP® MENTOR PROGRAM – SESSION TEN

DAD JOKE…

If you don't like it, it's Brad's fault!

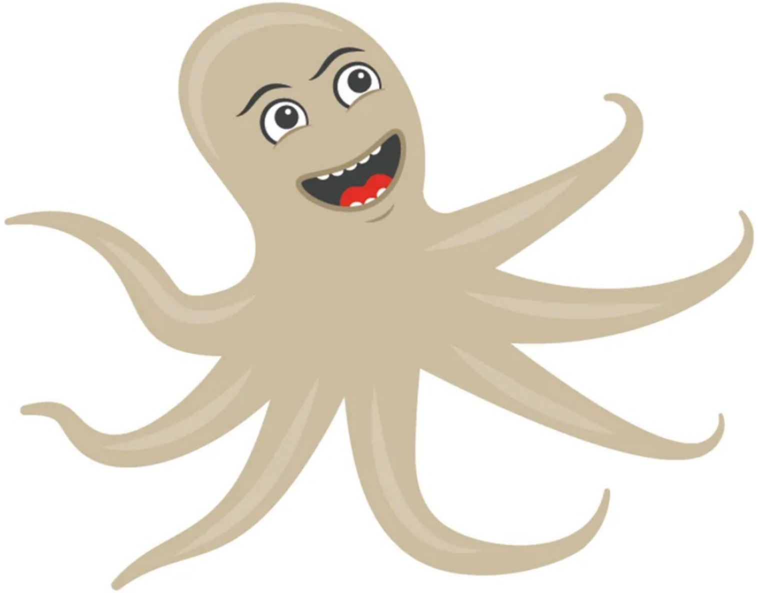
How many tickles does it take to make an octopus laugh?

DAD JOKE…

If you don't like it, it's Brad's fault!

How many tickles does it take to make an octopus laugh?

Ten Tickles!



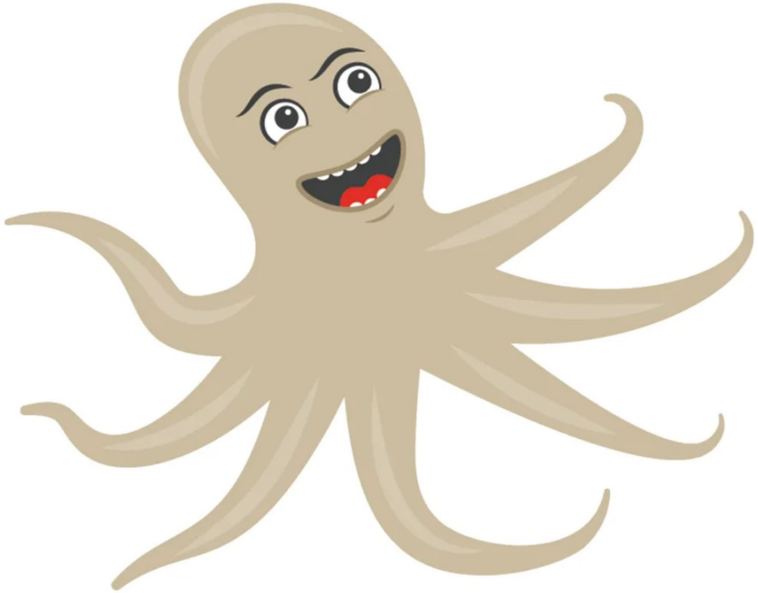
DAD JOKE…

If you don't like it, it's Brad's fault!

How many tickles does it take to make an octopus laugh?

Ten Tickles!

You get it right?!
Ten tickles, like tentacles.



DAD JOKE…

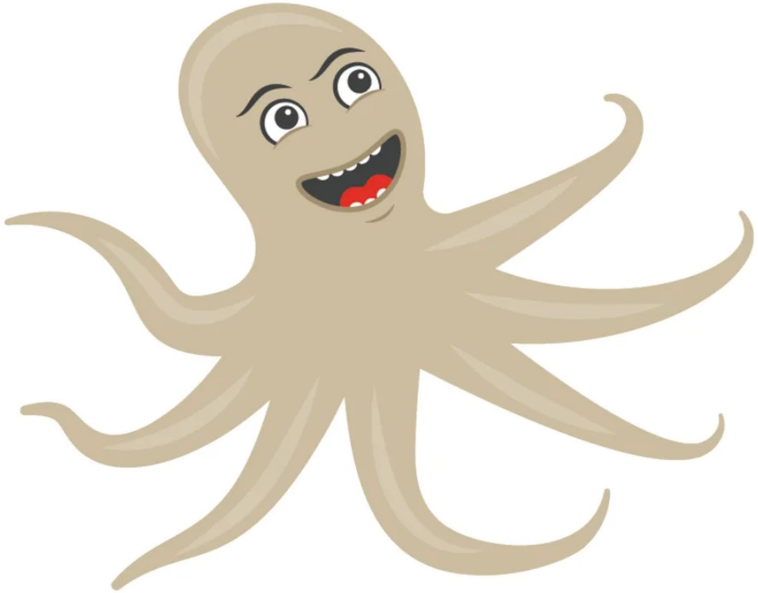
If you don’t like it, it’s Brad’s fault!

How many tickles does it take to make an octopus laugh?

Ten Tickles!

You get it right?!
Ten tickles, like tentacles.

Octopuses have tentacles! LOL!



DAD JOKE…

If you don't like it, it's Brad's fault!

How many tickles does it take to make an octopus laugh?

Ten Tickles!

You get it right?!
Ten tickles, like tentacles.

Octopuses have tentacles! LOL!

NO?
Whatever…

DOMAIN 7 – SECURITY OPERATIONS

Introduction

Security operations is about day-to-day operations and maintenance of the information security program.

- Also known as “SecOps”.
- If information security is “risk management”, SecOps is continual risk management.
- Take all the things you’ve learned so far and operationalize them.
- …and a little more.

CISSP® MENTOR PROGRAM – SESSION TEN

DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Topics include:

- Evidence collection and handling
- Reporting and documentation
- Investigative techniques
- Digital forensics tools, tactics, and procedures
- Artifacts (e.g., computer, network, mobile device)

It's important to get this right. A CISSP isn't expected to be a DFIR expert, but they must know the basics.

DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Evidence Collection and Handling

- Evidence supports something an assertion or proposition.
- The better the evidence, the better the support.
- There are four types evidence by which facts can be proven or disproven at trial which include:
  - Real evidence;
  - Demonstrative evidence;
  - Documentary evidence; and
  - Testimonial evidence.

https://www.findlaw.com/criminal/criminal-procedure/real-and-demonstrative-evidence.html

DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Evidence Collection and Handling

Real evidence

- often called physical evidence: material items involved in a case, objects and things a jury can physically hold and inspect. Examples of real evidence include fingerprints, blood samples, DNA, a knife, a gun, and other physical objects.
- Usually admitted because it tends to prove or disprove an issue of fact in a trial.
- In order to be used at trial, real evidence must be **relevant**, **material**, and **authentic**. **MUST** establish the item's chain of custody.

https://www.findlaw.com/criminal/criminal-procedure/real-and-demonstrative-evidence.html

DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Evidence Collection and Handling

Demonstrative Evidence

- Usually charts and diagrams, to demonstrate or illustrate the testimony of a witness.
- It's admissible when it fairly and accurately reflects the witness's testimony and is more probative than prejudicial. Maps, diagrams of a crime scene, charts and graphs that illustrate physical or financial injury to a plaintiff are examples of demonstrative evidence.
- Witnesses create and use demonstrative evidence at trial and opposing counsel may use the same evidence to prove contrary positions.

https://www.findlaw.com/criminal/criminal-procedure/real-and-demonstrative-evidence.html

DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Evidence Collection and Handling

Documentary Evidence

- The production of documents at trial is documentary evidence.
- Presented to prove or disprove certain allegations at trial.
- Documents can be from a vast number of sources from diaries, letters, contracts, newspapers, and any other type of document that you can think of.
- There are restrictions and qualifications for using documents at trial as there is a need to make sure they are authentic and trustworthy.

https://www.findlaw.com/criminal/criminal-procedure/real-and-demonstrative-evidence.html

DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Evidence Collection and Handling

Testimonial Evidence]

When a person gets up on the stand at trial and relates something that they saw or heard, that is testimonial evidence. It is simply a witness giving testimony under oath about the facts of the case.

https://www.findlaw.com/criminal/criminal-procedure/real-and-demonstrative-evidence.html

DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Evidence Collection and Handling

Testimonial Evidence]

When a person gets up on the stand at trial and relates something that they saw or heard, that is testimonial evidence. It is simply a witness giving testimony under oath about the facts of the case.

OK, back to our regularly scheduled programming…

https://www.findlaw.com/criminal/criminal-procedure/real-and-demonstrative-evidence.html

DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Collecting Digital Evidence

- The integrity of the evidence is CRITICAL!
- Rule of Thumb – IF YOU'RE GOING TO FAST TO DOCUMENT EVERYTHING, THEN YOU'RE GOING TO FAST.
- Document dates, times, physical locations, logical locations, all actions that were taken, observations, etc. TIP: Take pictures too.
- NEVER tamper with original versions of anything. ALWAYS make write-block, make bit-level copies, and investigate on the copies. TIP: Make two copies and store the original safely.

ERATIONS

nvestigations

I prefer hardware write-blockers.

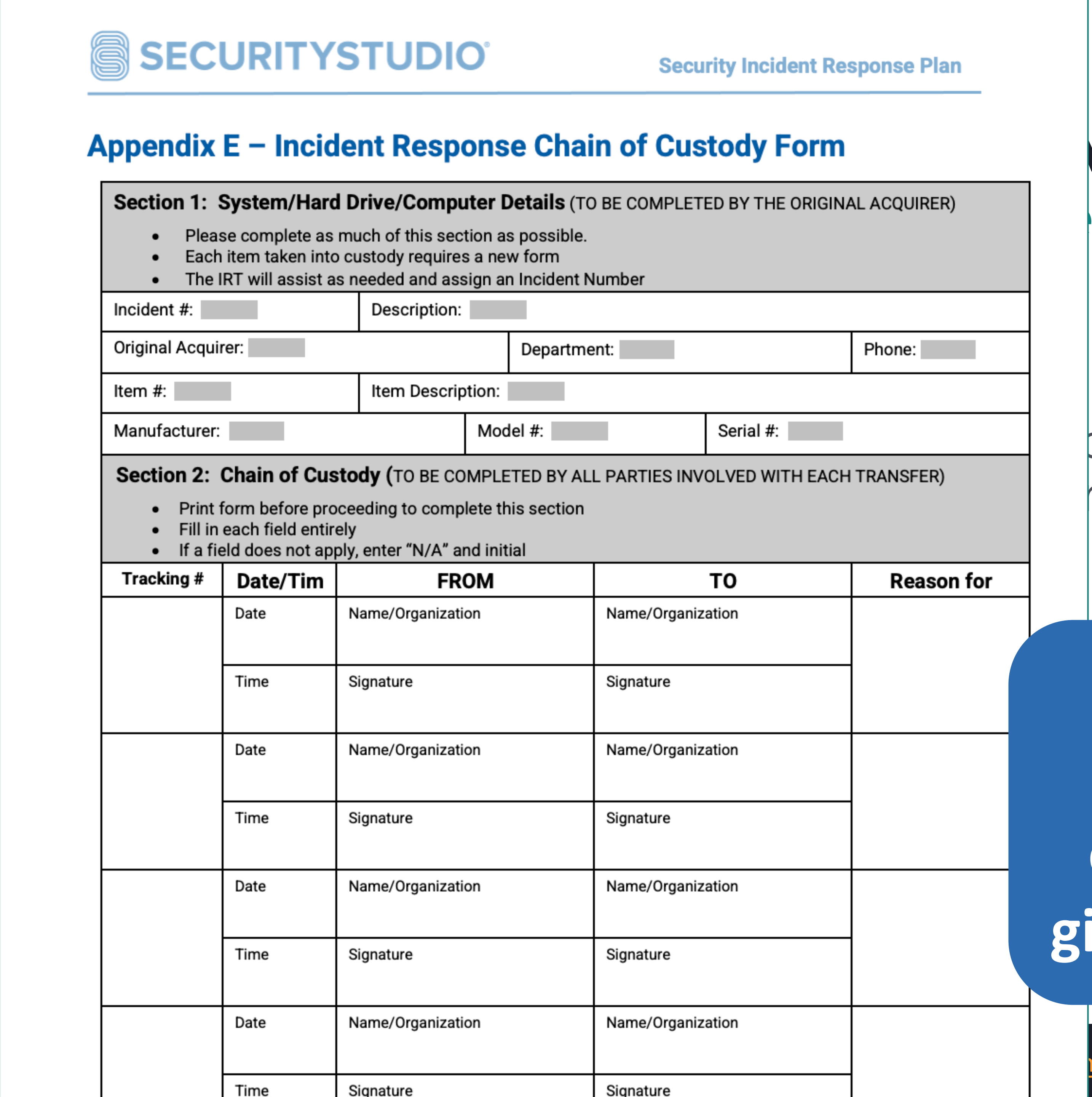
DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Handling Digital Evidence

- Did I mention **integrity**?!
- Every second must be accounted for from the second you encounter evidence until you no longer have any contact with the evidence.
- Chain of Custody must be maintained.
- A well-known standard: **ISO/IEC 27037:2012**, "*Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*"

#MissionBeforeMoney



SECURITYSTUDIO®

Security Incident Response Plan

Appendix E – Incident Response Chain of Custody Form

Section 1: System/Hard Drive/Computer Details (TO BE COMPLETED BY THE ORIGINAL ACQUIRER)

- Please complete as much of this section as possible.
- Each item taken into custody requires a new form
- The IRT will assist as needed and assign an Incident Number

Incident #:

Description:

Original Acquirer:

Department:

Phone:

Item #:

Item Description:

Manufacturer:

Model #:

Serial #:

Section 2: Chain of Custody (TO BE COMPLETED BY ALL PARTIES INVOLVED WITH EACH TRANSFER)

- Print form before proceeding to complete this section
- Fill in each field entirely
- If a field does not apply, enter "N/A" and initial

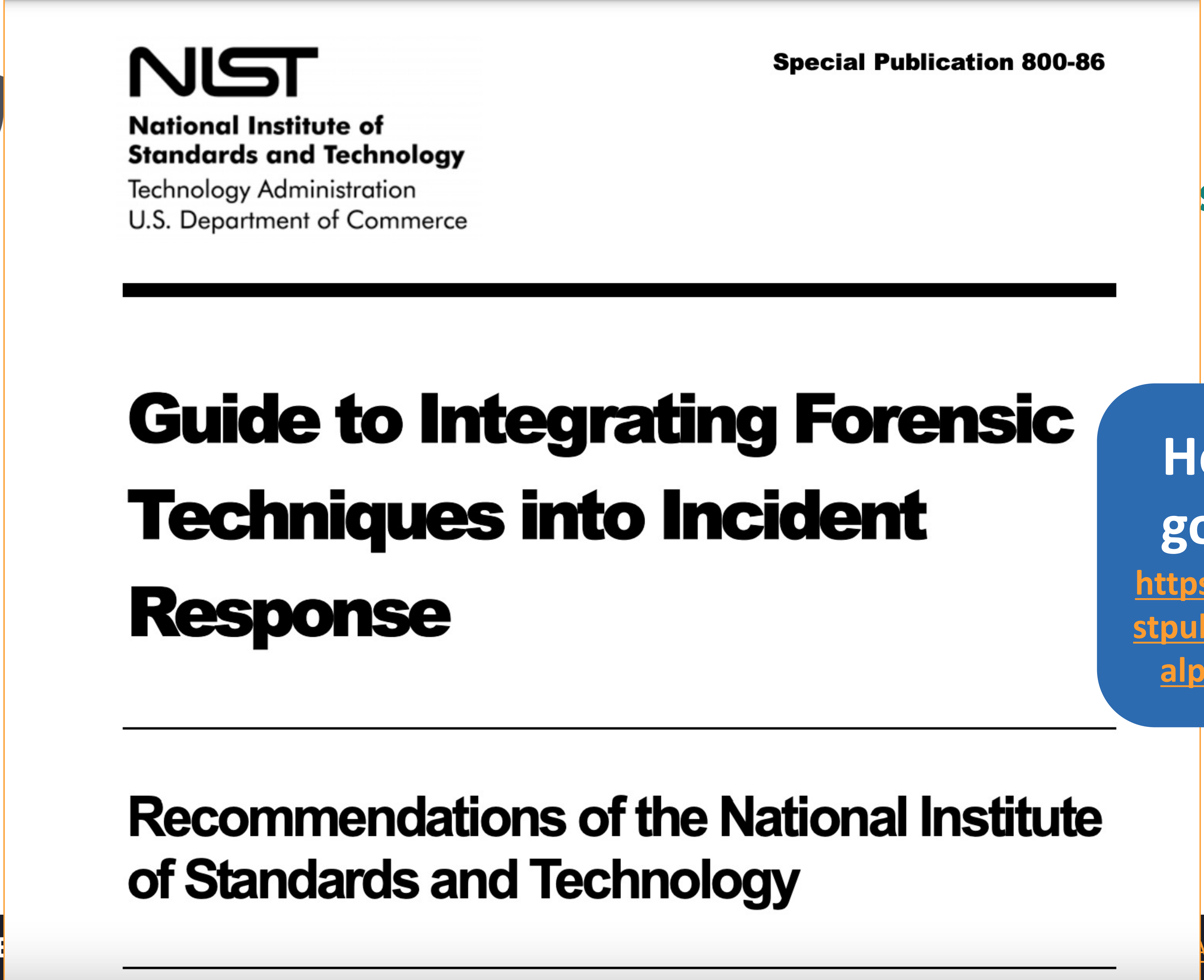
Tracking #	Date/Tim	FROM	TO	Reason for
	Date	Name/Organization	Name/Organization	
	Time	Signature	Signature	
	Date	Name/Organization	Name/Organization	
	Time	Signature	Signature	
	Date	Name/Organization	Name/Organization	
	Time	Signature	Signature	
	Date	Name/Organization	Name/Organization	
	Time	Signature	Signature	

TIONS

stigations

om the second you
r have any contact

I'll post a copy for your reading enjoyment. We like giving away free stuff!



NIST

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

Special Publication 800-86

Guide to Integrating Forensic Techniques into Incident Response

Recommendations of the National Institute of Standards and Technology

Here's another good resource.
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Reporting and Documentation

- Again, document **EVERYTHING**.
- As much as possible, avoid subjective interpretations and space for subjective interpretations.
- As much as possible, ensure evidence is admissible (even if you’re not sure that your evidence will be presented in court).

DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Reporting and Documentation

Admissibility of Evidence:

- **Accuracy** – lacking errors.
- **Authenticity** - undisputed origin.
- **Comprehensibility** – paint as much of the picture as possible.
- **Convincing** – certainty in conclusions.
- **Objective** – what the evidence says, not what you say. Facts versus opinions.
- **Admissible** – for the court in question.

CISSP® MENTOR PROGRAM – SESSION TEN

DOMAIN 7 – SECURITY OPERATIONS

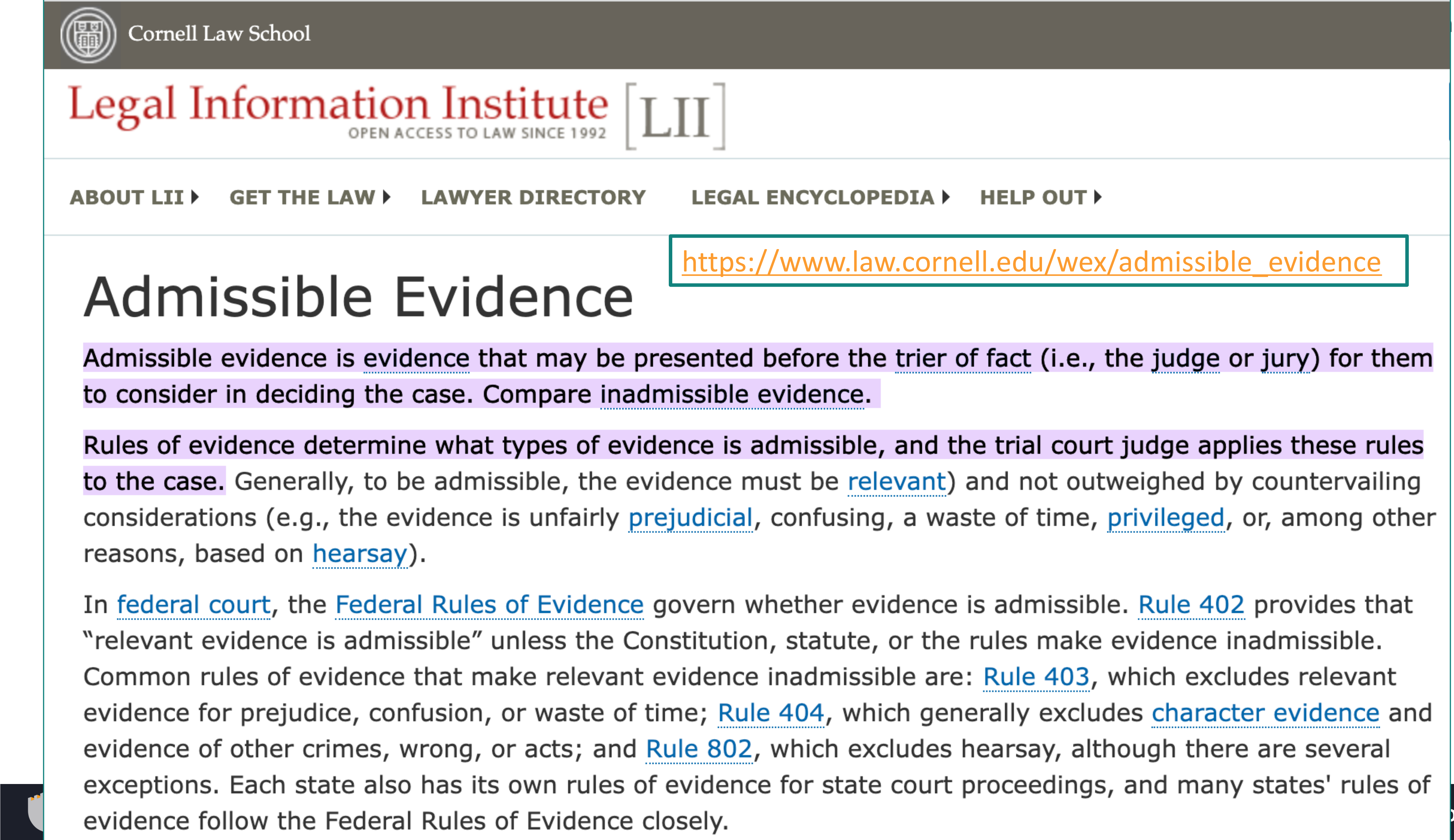
Understand and comply with investigations

Reporting and Documentation

Admissibility of Evidence:

- **Accuracy** –
- **Authentici**
- **Comprehe** possible.
- **Convincing**
- **Objective** – versus opinions.
- **Admissible** – for the court in question.

Seek advice from legal counsel, law enforcement, or other investigative professionals to ensure evidence you collect, handle, and prepare is adequate ey



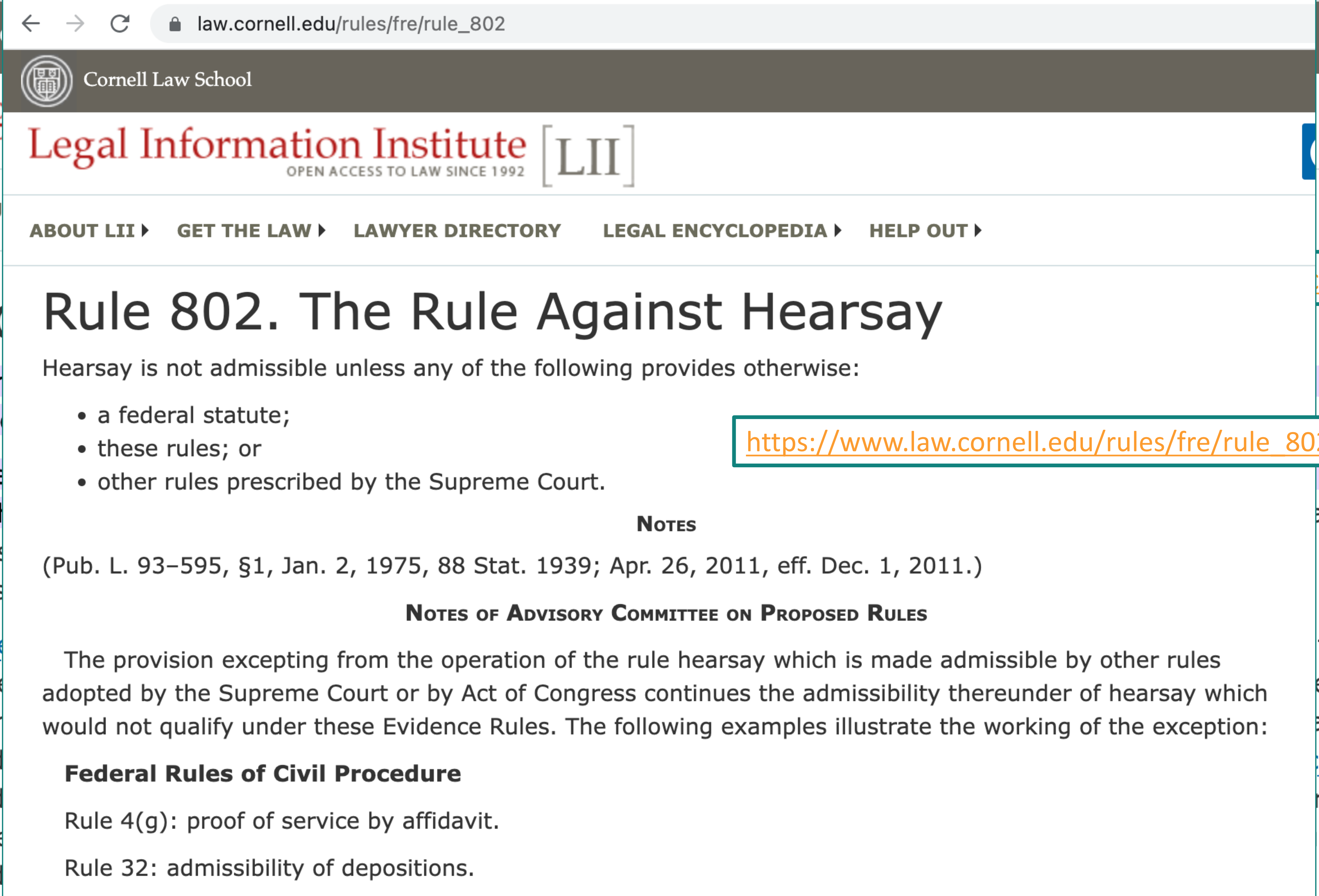
https://www.law.cornell.edu/wex/admissible_evidence

Admissible Evidence

Admissible evidence is evidence that may be presented before the trier of fact (i.e., the judge or jury) for them to consider in deciding the case. Compare inadmissible evidence.

Rules of evidence determine what types of evidence is admissible, and the trial court judge applies these rules to the case. Generally, to be admissible, the evidence must be relevant) and not outweighed by countervailing considerations (e.g., the evidence is unfairly prejudicial, confusing, a waste of time, privileged, or, among other reasons, based on hearsay).

In federal court, the Federal Rules of Evidence govern whether evidence is admissible. Rule 402 provides that “relevant evidence is admissible” unless the Constitution, statute, or the rules make evidence inadmissible. Common rules of evidence that make relevant evidence inadmissible are: Rule 403, which excludes relevant evidence for prejudice, confusion, or waste of time; Rule 404, which generally excludes character evidence and evidence of other crimes, wrong, or acts; and Rule 802, which excludes hearsay, although there are several exceptions. Each state also has its own rules of evidence for state court proceedings, and many states' rules of evidence follow the Federal Rules of Evidence closely.



law.cornell.edu/rules/fre/rule_802
Cornell Law School
Legal Information Institute [LII]
OPEN ACCESS TO LAW SINCE 1992
ABOUT LII ▸
GET THE LAW ▸
LAWYER DIRECTORY
LEGAL ENCYCLOPEDIA ▸
HELP OUT ▸

Rule 802. The Rule Against Hearsay

Hearsay is not admissible unless any of the following provides otherwise:

- a federal statute;
- these rules; or
- other rules prescribed by the Supreme Court.

Notes

(Pub. L. 93–595, §1, Jan. 2, 1975, 88 Stat. 1939; Apr. 26, 2011, eff. Dec. 1, 2011.)

Notes of Advisory Committee on Proposed Rules

The provision excepting from the operation of the rule hearsay which is made admissible by other rules adopted by the Supreme Court or by Act of Congress continues the admissibility thereunder of hearsay which would not qualify under these Evidence Rules. The following examples illustrate the working of the exception:

Federal Rules of Civil Procedure

Rule 4(g): proof of service by affidavit.

Rule 32: admissibility of depositions.

https://www.law.cornell.edu/rules/fre/rule_802

DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Investigative Techniques

Four main techniques

- **Data capture** – manual and automatic capture.
- **Interviews** – ideally from someone who was a witness to an incident or a person with first-hand knowledge of the incident.
- **Interrogations** – usually done by law enforcement following stringent rules.
- **External requests** – usually warrants and subpoenas.

DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Investigative Techniques

Four main techniques

- **Data capture** – manual and automatic capture.
- **Inte**… an inci… inci…
- **Interrogations** – usually done by law enforcement following stringent…
- **External requests** – usually warrants and subpoenas.

Let the evidence draw your conclusions. If the evidence isn’t available (coming later), you may not be able to draw conclusions.

When in question, leave it to the experts.

DOMAIN 7 – SECURITY OPERATIONS

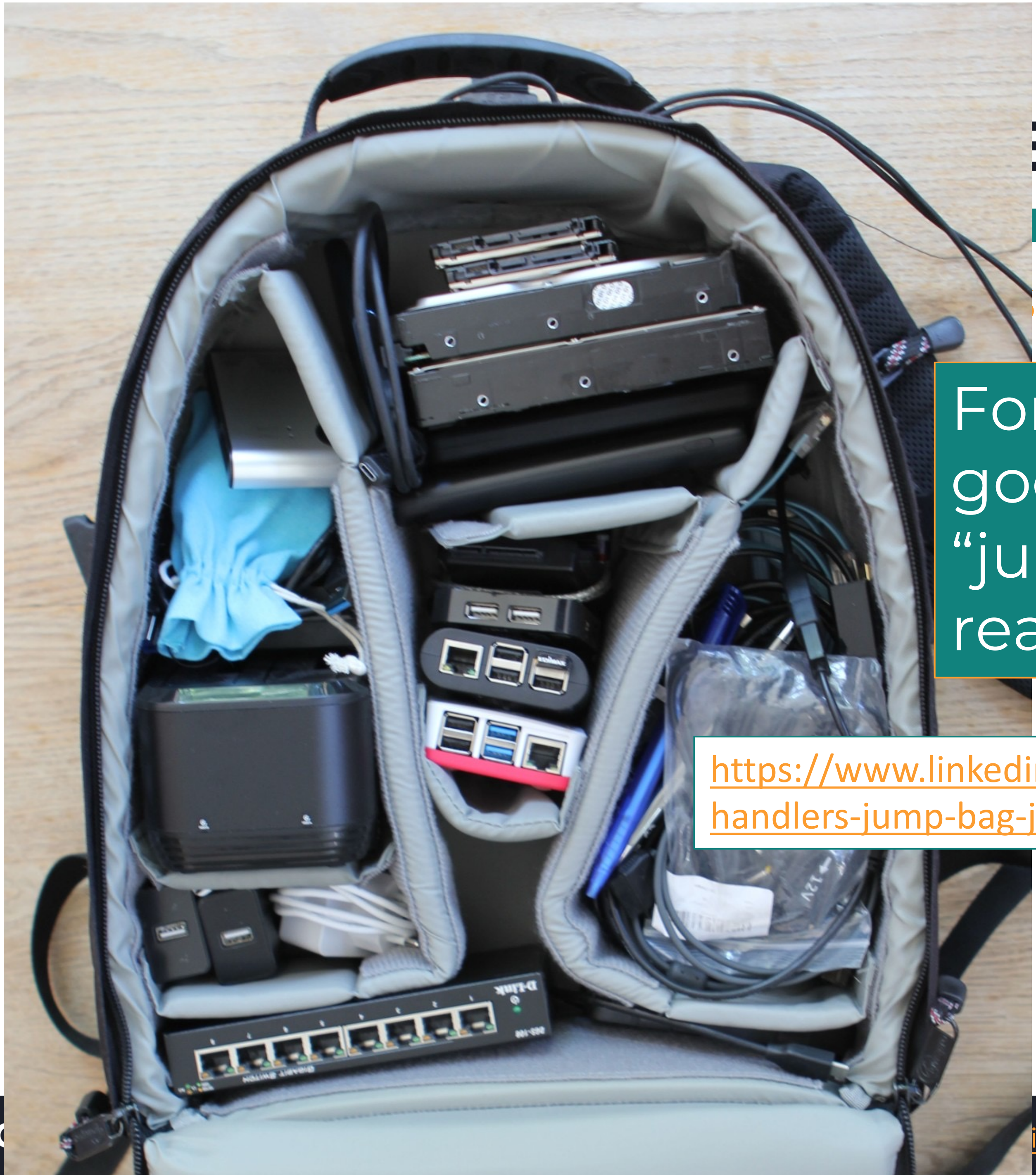
Understand and comply with investigations

Digital Forensics Tools, Tactics, and Procedures

ERATIONS

nvestigations

, and Procedures



Forensics investigators (the good ones) have a "jumpbag" with their tools ready to use.

https://www.linkedin.com/pulse/cyber-security-incident-handlers-jump-bag-jean-francois-stenuit/

DOMAIN 7 – SECURITY OPERATIONS

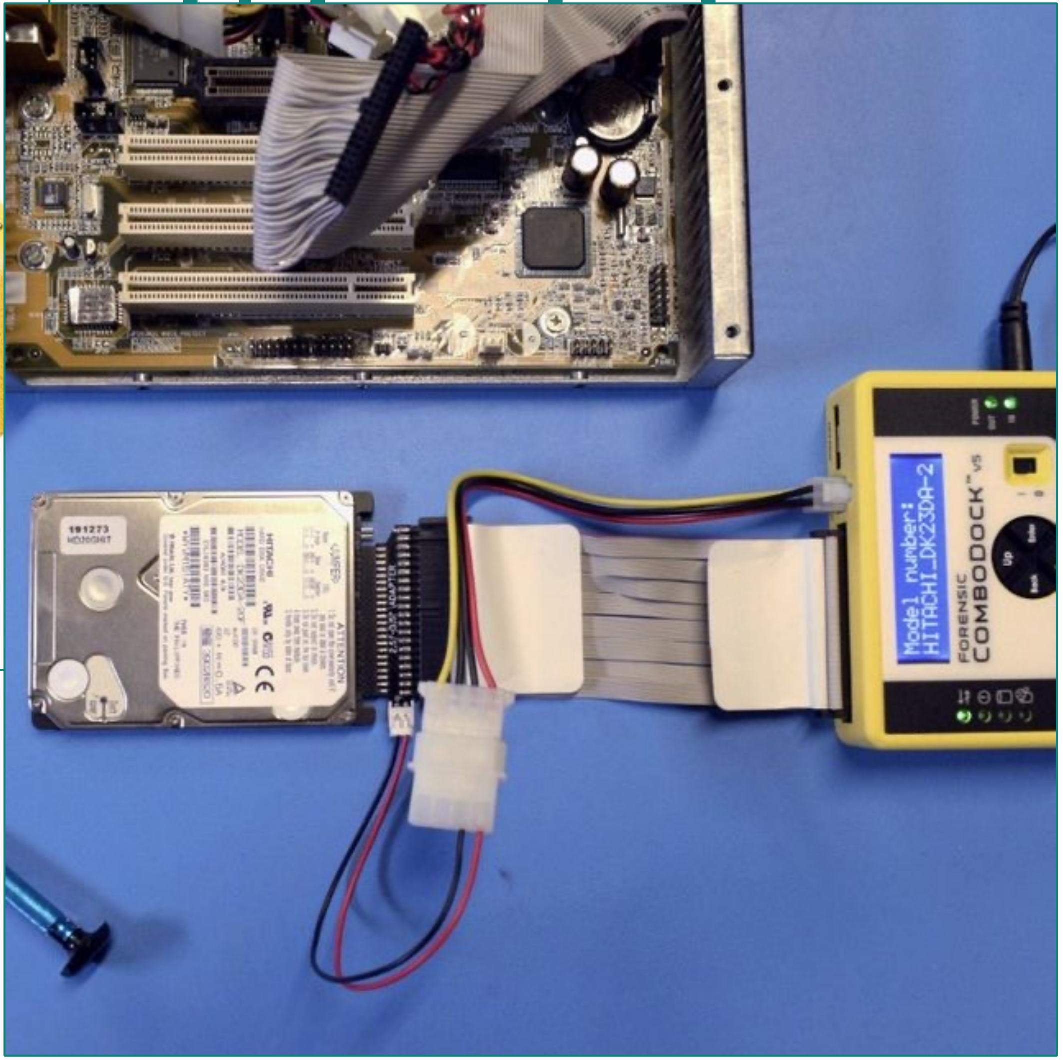
Understand and comply with investigations

Digital Forensics Tools, Tactics, and Procedures

Write blockers and drive imagers

designed to allow examination or imaging of a storage device, typically a hard drive, without writing any data to the storage device, which would violate the integrity of the evidence.

TY OPERATIONS



DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Digital Forensics Tools, Tactics, and Procedures

Faraday containers

Protects evidence from electromagnetic interference.

SESSION TEN

CURITY OPERATIONS

comply with investigations

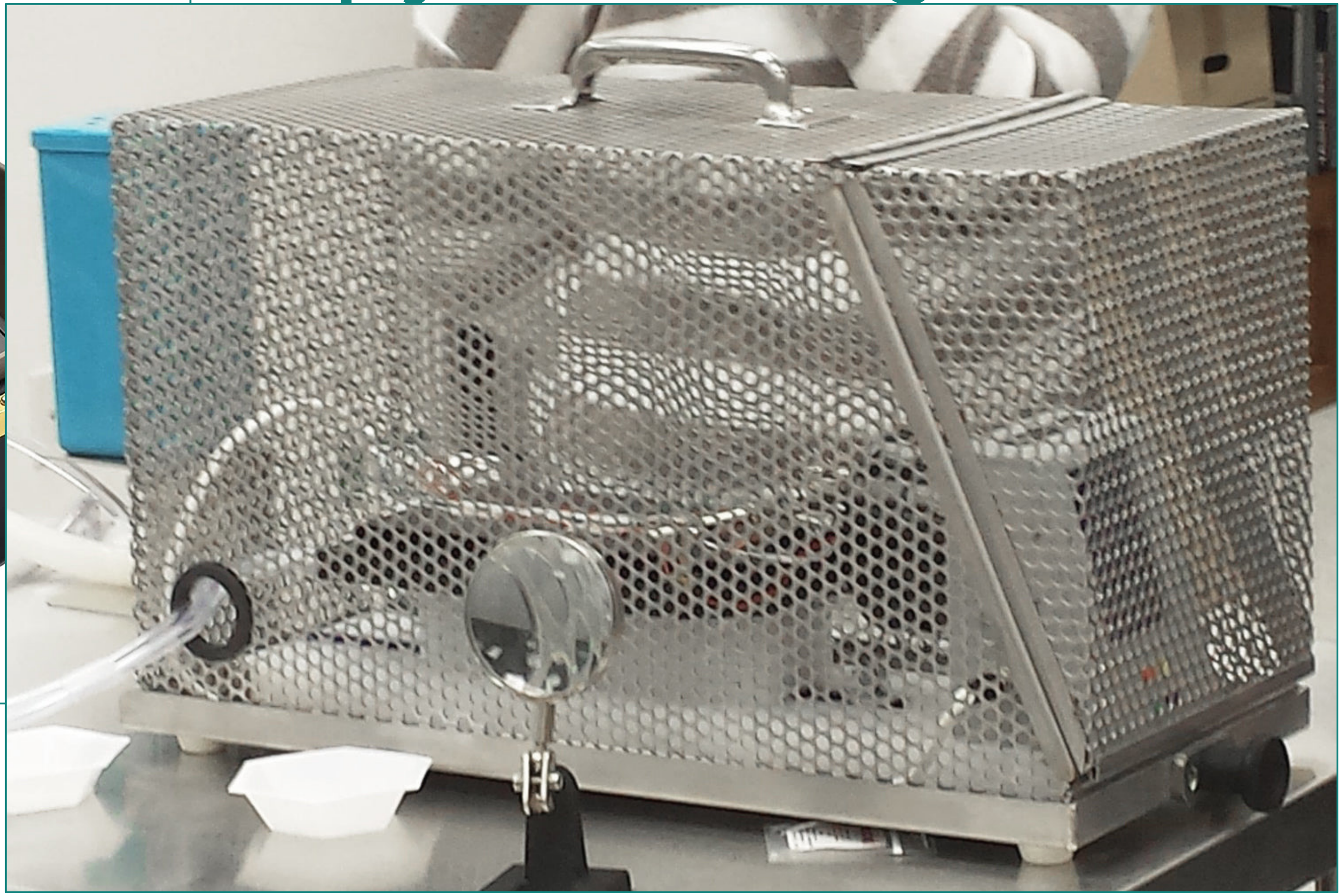
Tools, Tactics, and Procedures

om electromagnetic interference.

SESSION TEN

CURITY OPERATIONS

comply with investigations



SESSION TEN

CURITY OP

comply with

DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Digital Forensics Tools, Tactics, and Procedures

Video and audio recording tools

I've heard it in court before, "video doesn't lie". Might be sorta true, but video and audio can be very compelling. Can save a lot of time during an investigation too.

In general, Secure the physical "crime scene" first.

DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Digital Forensics Tools, Tactics, and Procedures

- **Network traffic analysis** tools - Wireshark (and similar) for pcap and analysis.
- **Log analysis** tools - SIEM (and similar) to reconstruct events across systems and for context.
- **Data recovery** tools – file recovery for things deleted or overwritten
- Virtual machines – useful for rebuilding (isolated) environments.
- **Code analysis** tools - decompilers and reverse-engineer software.
- **Hashing** tools – integrity verification.
- **Toolkits** – software suite specifically designed for forensic investigations.

ONS

gations

rocedures

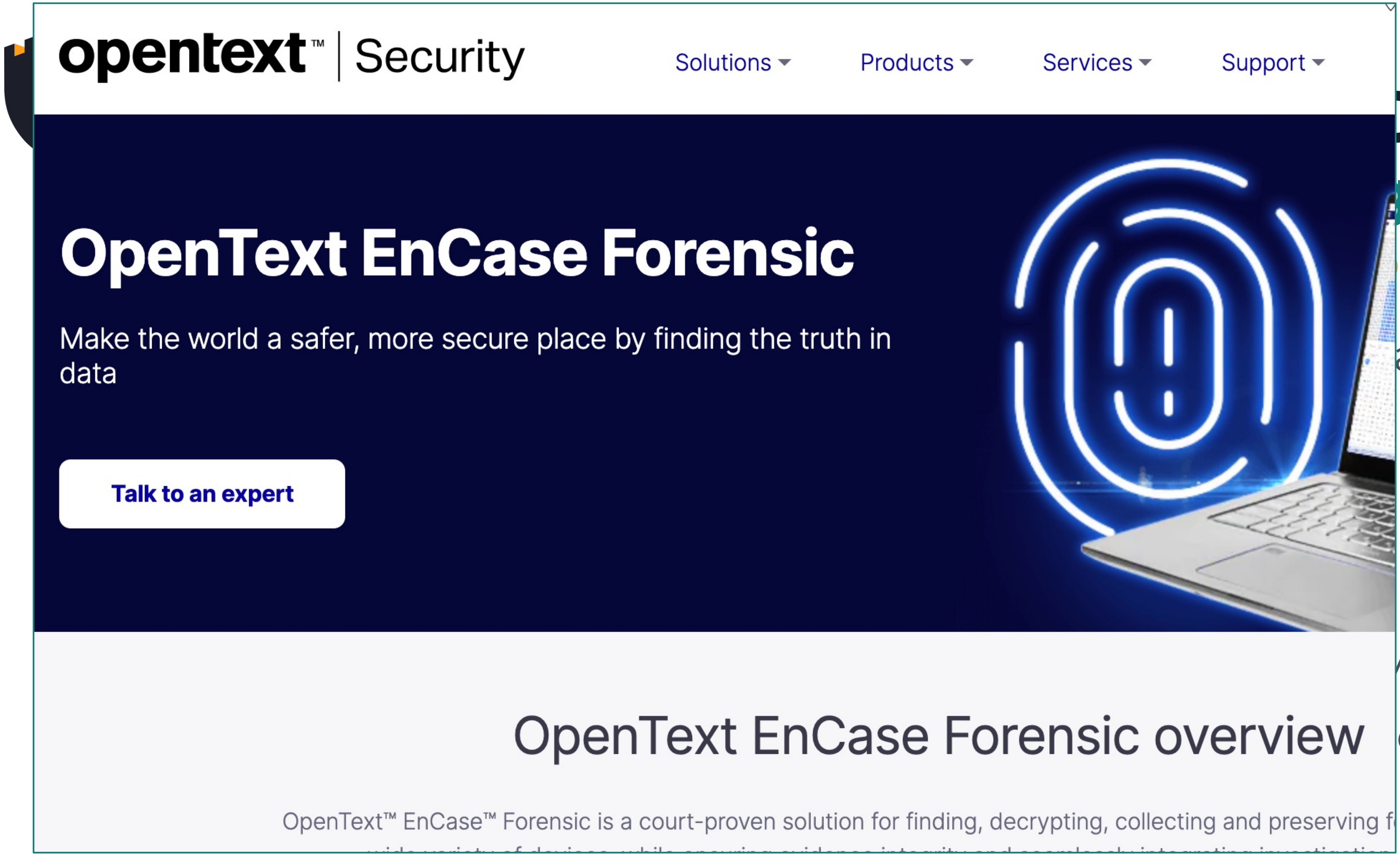
ar) for pcap and

events across

or overwritten

ironments.

eer software.



OpenText EnCase Forensic

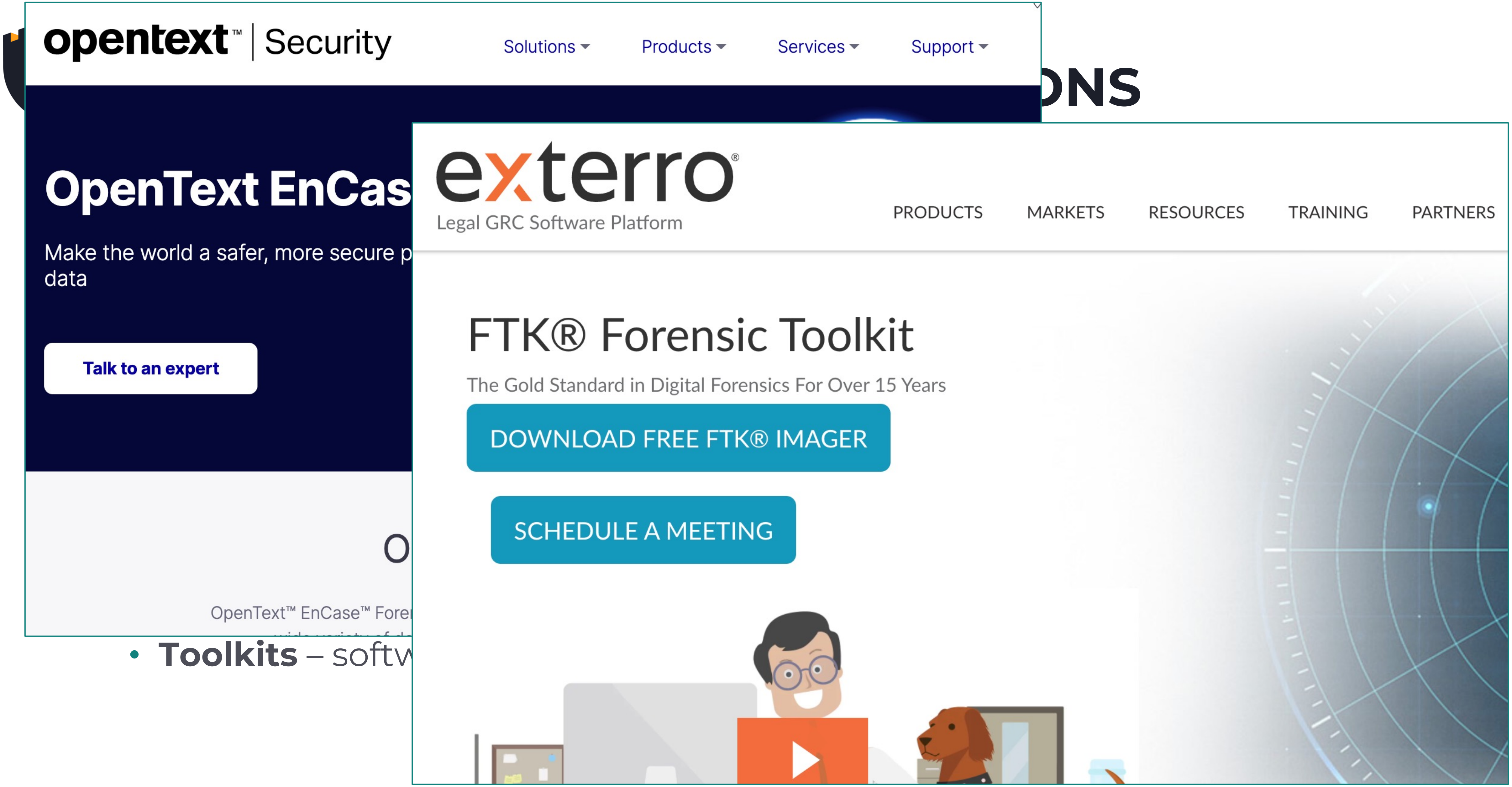
Make the world a safer, more secure place by finding the truth in data

OpenText EnCase Forensic overview

OpenText™ EnCase™ Forensic is a court-proven solution for finding, decrypting, collecting and preserving f

- **Toolkits** – software suite specifically designed for forensic investigations.

ONS



OpenText EnCas

Make the world a safer, more secure p
data

O

OpenText™ EnCase™ Fore

FTK® Forensic Toolkit

The Gold Standard in Digital Forensics For Over 15 Years

- **Toolkits** – softw

DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Digital Forensics Tools, Tactics, and Procedures

Techniques and Procedures

- Digital forensics is a specialized skill.
- Strict procedures should be prepared ahead of time and followed for conducting a forensic investigation.
- Either part of an incident response (IR) plan or a supplement to an IR plan.
- Documented standards for the collection, handling, and investigation of digital evidence include ISO 27041, 27042, 27043, and 27050
- SANS - https://www.sans.org/posters/?focus-area=digital-forensics

CISSP® MENTOR PROGRAM – SESSION TEN

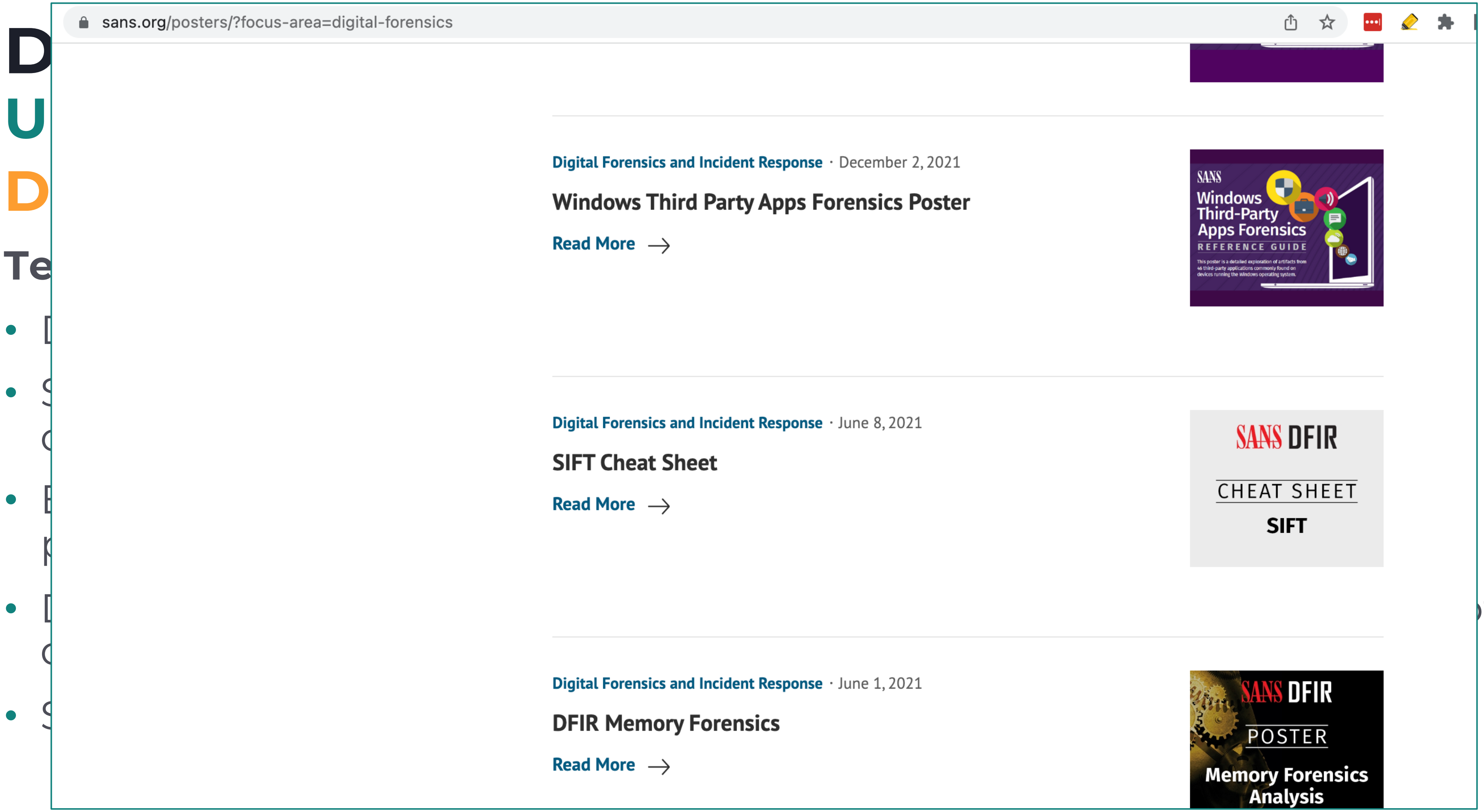
D

U

D

Te

- [
- S
  C
- E
  p
- [
  C
  of
- S



sans.org/posters/?focus-area=digital-forensics

Digital Forensics and Incident Response · December 2, 2021

Windows Third Party Apps Forensics Poster

Read More →

Digital Forensics and Incident Response · June 8, 2021

SIFT Cheat Sheet

Read More →

Digital Forensics and Incident Response · June 1, 2021

DFIR Memory Forensics

Read More →

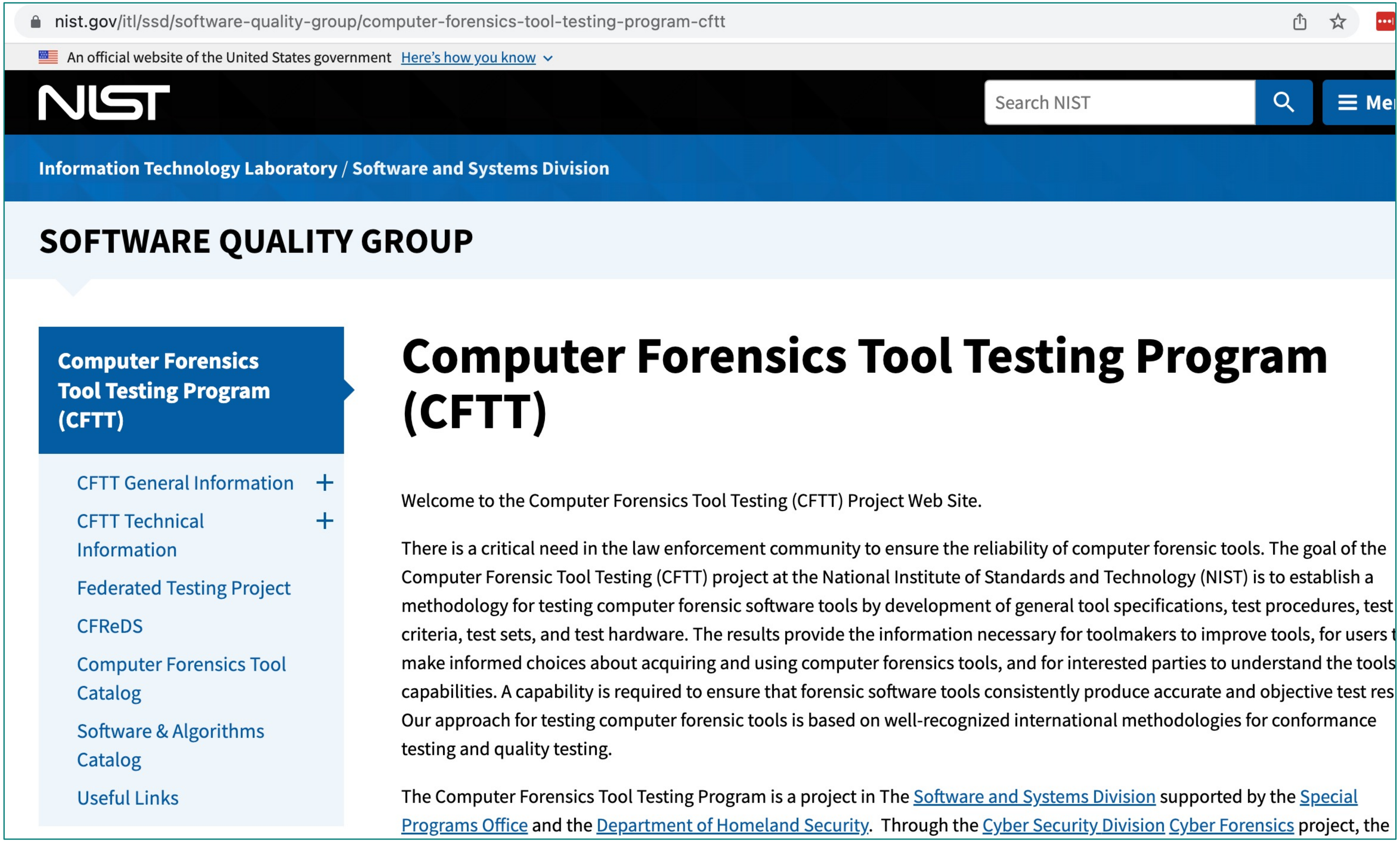
DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Digital Forensics Tools, Tactics, and Procedures

Techniques and Procedures

- Digital forensics is a specialized skill.
- Strict procedures should be prepared ahead of time and followed for conducting a forensic investigation.
- Either part of an incident response (IR) plan or a supplement to an IR plan.
- Documented standards for the collection, handling, and investigation of digital evidence include ISO 27041, 27042, 27043, and 27050
- SANS - https://www.sans.org/posters/?focus-area=digital-forensics
- NIST Computer Forensics Tool Testing Program (CFTT) site: nist.gov/itl/ssd/software- quality-group/computer-forensics-tool-testing-program-cftt



nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt
An official website of the United States government Here's how you know
NIST
Search NIST
Me
Information Technology Laboratory / Software and Systems Division

SOFTWARE QUALITY GROUP

Computer Forensics Tool Testing Program (CFTT)

- CFTT General Information +
- CFTT Technical Information +
- Federated Testing Project
- CFReDS
- Computer Forensics Tool Catalog
- Software & Algorithms Catalog
- Useful Links

Computer Forensics Tool Testing Program (CFTT)

Welcome to the Computer Forensics Tool Testing (CFTT) Project Web Site.

There is a critical need in the law enforcement community to ensure the reliability of computer forensic tools. The goal of the Computer Forensic Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) is to establish a methodology for testing computer forensic software tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware. The results provide the information necessary for toolmakers to improve tools, for users t make informed choices about acquiring and using computer forensics tools, and for interested parties to understand the tools capabilities. A capability is required to ensure that forensic software tools consistently produce accurate and objective test res Our approach for testing computer forensic tools is based on well-recognized international methodologies for conformance testing and quality testing.

The Computer Forensics Tool Testing Program is a project in The Software and Systems Division supported by the Special Programs Office and the Department of Homeland Security. Through the Cyber Security Division Cyber Forensics project, the

DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Digital Forensics Tools, Tactics, and Procedures

Techniques and Procedures (generic procedure steps in book)

1. Define priorities
2. Identify data sources
3. Plan to collect data and execute
4. Document and preserve integrity
5. Look for hidden or erased data
6. Perform analysis

In reality, you are performing analysis continually (so this is not serial). **ALWAYS** let the evidence (and logic) lead the investigation. Do **NOT** make assumptions whenever possible.

CISSP® MENTOR PROGRAM – SESSION TEN

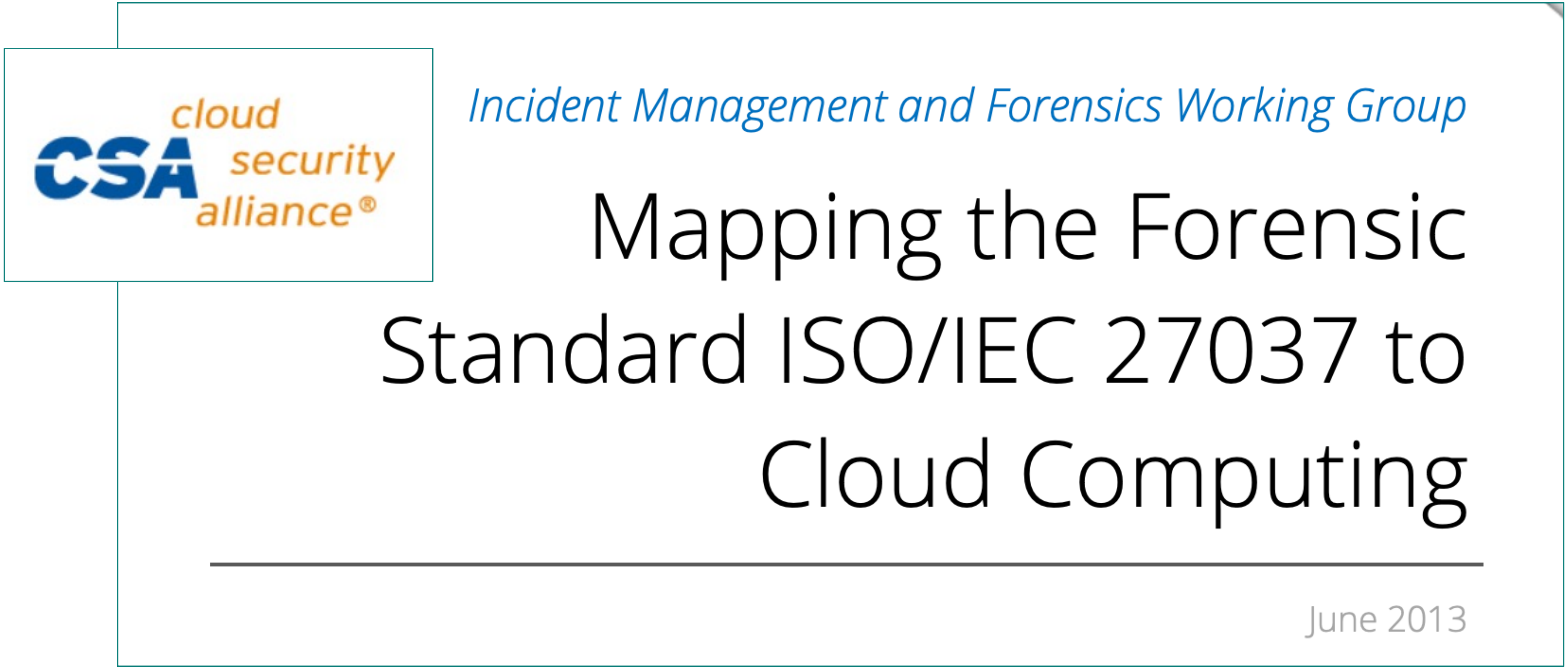
DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Digital Forensics Tools, Tactics, and Procedures

Cloud-Specific

DOMAIN 7 – SECURITY OPERATIONS



cloud security alliance®

CSA

Incident Management and Forensics Working Group

Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing

June 2013

CISSP® MENTOR PROGRAM – SESSION TEN

DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

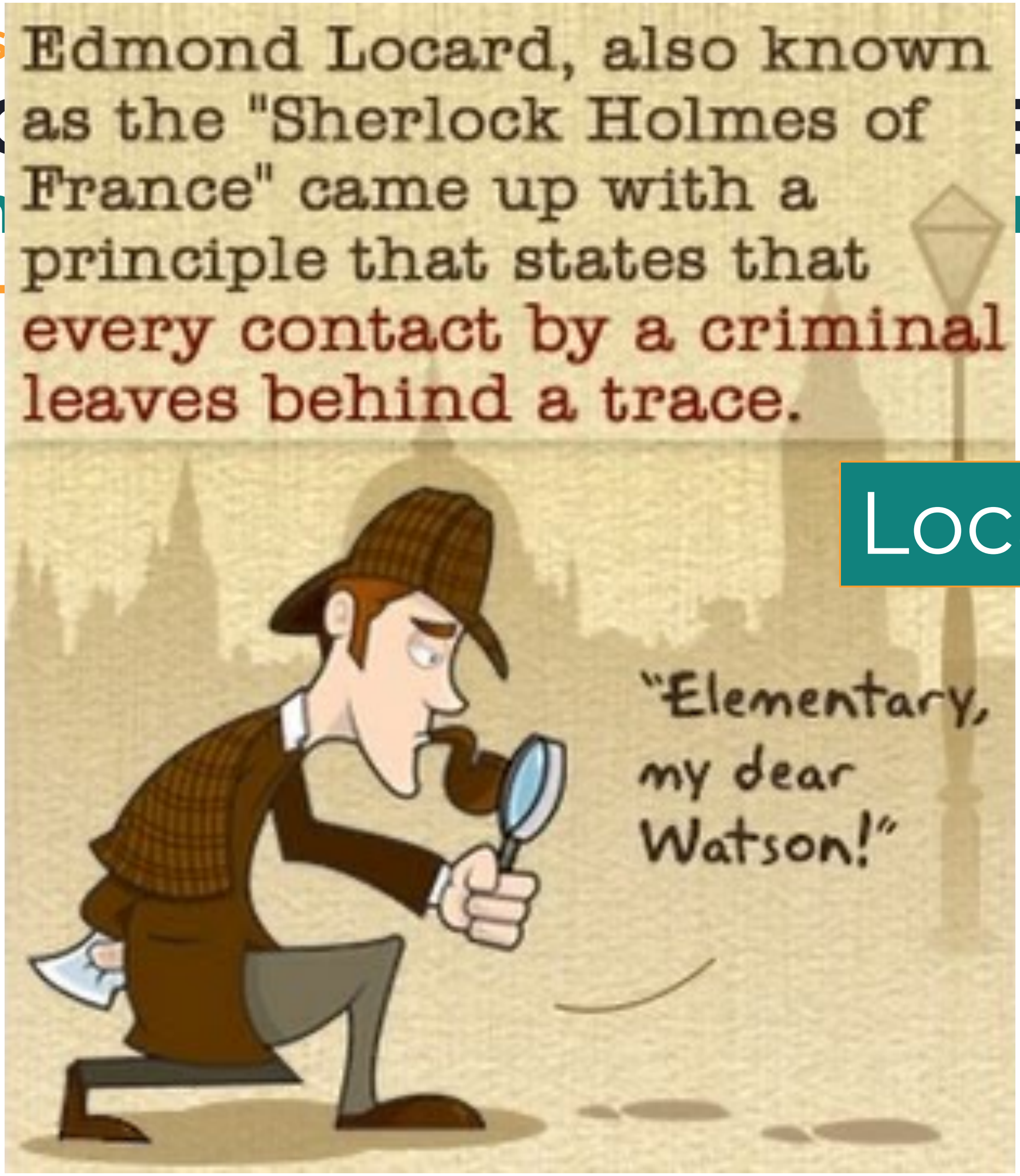
Artifacts

CISS

DC ERATIONS

Un nvestigations

Ar



Edmond Locard, also known as the "Sherlock Holmes of France" came up with a principle that states that every contact by a criminal leaves behind a trace.

Locard's Principle

DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Artifacts – Computers (Sources)

Specifics matter.

Windows

Logs (Event Viewer and others), Recycle Bin, Registry, etc.

Apple macOS

Logs (Console and others), Trash, Time Machine, property list (PLIST) files.

Linux

/usr folder, /tmp (volatile temporary files), /var (caches, log files, and information about currently running processes).

DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Artifacts – Computers (Sources)

Specifics matter.

Browsers

Cache, history, cookies, etc.

Local Storage

File remnants, deleted files, file movement, etc.

Cloud Storage

Not unlike local storage, but investigators typically don't have the same level of access; therefore, requests are made informally and/or formally of cloud providers.

DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Artifacts – Network (Sources)

Specifics matter.

NetFlow

Collect IP network traffic as it enters or exits interfaces. A network administrator can determine the source and destination of traffic, class of service, data types, etc.

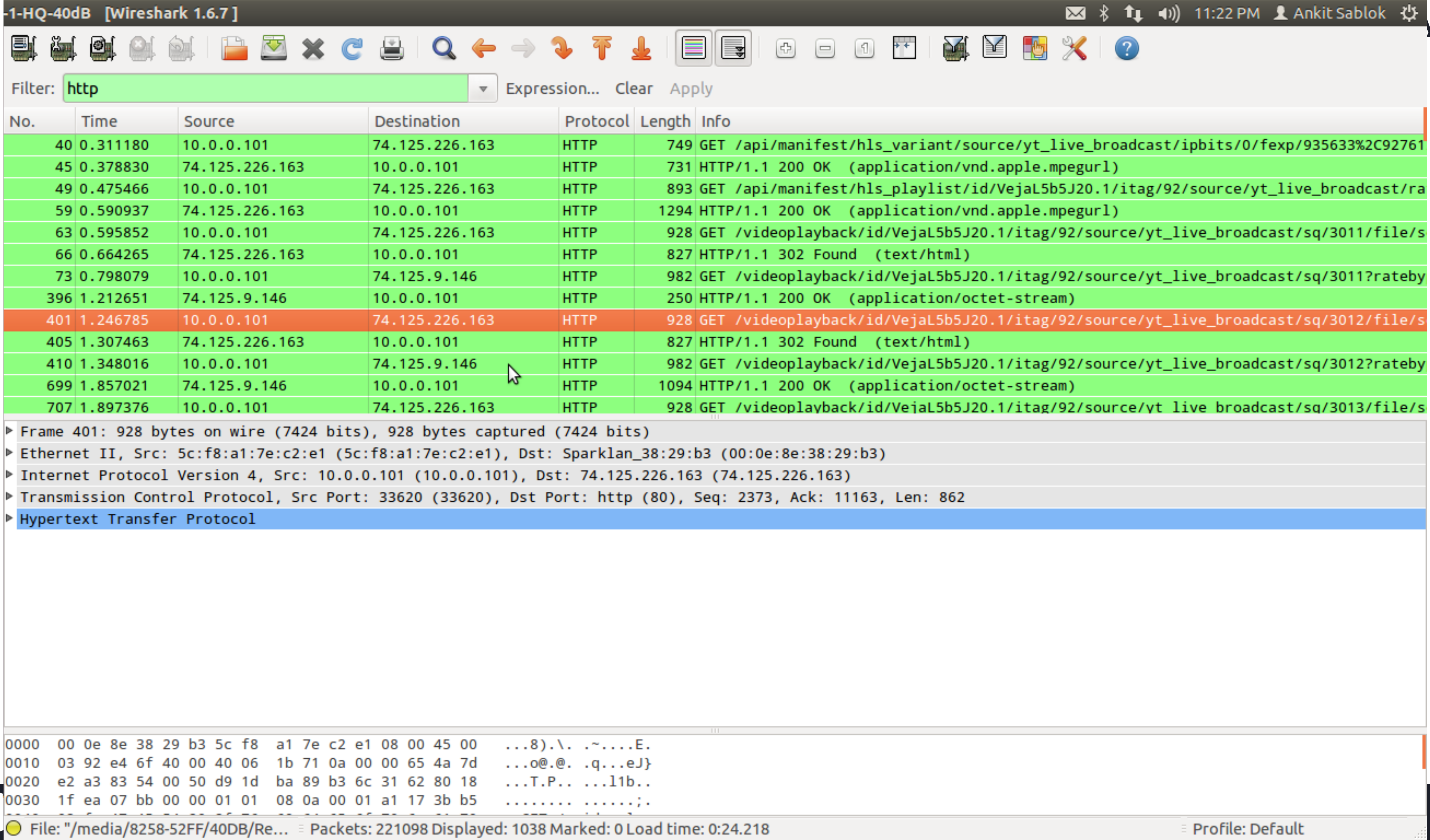
Packet analysis (pcap)

Captures details about communications and the data itself.

Known bad traffic (block list)

C2 traffic, known malicious sites, etc. This one is big for IoCs.

Network device log files



Filter: http

```
No.  Time      Source          Destination     Protocol Length Info
  40 0.311180  10.0.0.101      74.125.226.163  HTTP      749 GET /api/manifest/hls_variant/source/yt_live_broadcast/ipbits/0/fexp/935633%2C92761
  45 0.378830  74.125.226.163  10.0.0.101      HTTP      731 HTTP/1.1 200 OK  (application/vnd.apple.mpegurl)
  49 0.475466  10.0.0.101      74.125.226.163  HTTP      893 GET /api/manifest/hls_playlist/id/VejaL5b5J20.1/itag/92/source/yt_live_broadcast/ra
  59 0.590937  74.125.226.163  10.0.0.101      HTTP     1294 HTTP/1.1 200 OK  (application/vnd.apple.mpegurl)
  63 0.595852  10.0.0.101      74.125.226.163  HTTP      928 GET /videoplayback/id/VejaL5b5J20.1/itag/92/source/yt_live_broadcast/sq/3011/file/s
  66 0.664265  74.125.226.163  10.0.0.101      HTTP      827 HTTP/1.1 302 Found  (text/html)
  73 0.798079  10.0.0.101      74.125.9.146    HTTP      982 GET /videoplayback/id/VejaL5b5J20.1/itag/92/source/yt_live_broadcast/sq/3011?rateby
 396 1.212651  74.125.9.146    10.0.0.101      HTTP      250 HTTP/1.1 200 OK  (application/octet-stream)
 401 1.246785  10.0.0.101      74.125.226.163  HTTP      928 GET /videoplayback/id/VejaL5b5J20.1/itag/92/source/yt_live_broadcast/sq/3012/file/s
 405 1.307463  74.125.226.163  10.0.0.101      HTTP      827 HTTP/1.1 302 Found  (text/html)
 410 1.348016  10.0.0.101      74.125.9.146    HTTP      982 GET /videoplayback/id/VejaL5b5J20.1/itag/92/source/yt_live_broadcast/sq/3012?rateby
 699 1.857021  74.125.9.146    10.0.0.101      HTTP     1094 HTTP/1.1 200 OK  (application/octet-stream)
 707 1.897376  10.0.0.101      74.125.226.163  HTTP      928 GET /videoplayback/id/VejaL5b5J20.1/itag/92/source/yt_live_broadcast/sq/3013/file/s
```

```
▶ Frame 401: 928 bytes on wire (7424 bits), 928 bytes captured (7424 bits)
▶ Ethernet II, Src: 5c:f8:a1:7e:c2:e1 (5c:f8:a1:7e:c2:e1), Dst: Sparklan_38:29:b3 (00:0e:8e:38:29:b3)
▶ Internet Protocol Version 4, Src: 10.0.0.101 (10.0.0.101), Dst: 74.125.226.163 (74.125.226.163)
▶ Transmission Control Protocol, Src Port: 33620 (33620), Dst Port: http (80), Seq: 2373, Ack: 11163, Len: 862
▶ Hypertext Transfer Protocol
```

```
0000  00 0e 8e 38 29 b3 5c f8  a1 7e c2 e1 08 00 45 00   ...8).\. .~....E.
0010  03 92 e4 6f 40 00 40 06  1b 71 0a 00 00 65 4a 7d   ...o@.@. .q...eJ}
0020  e2 a3 83 54 00 50 d9 1d  ba 89 b3 6c 31 62 80 18   ...T.P.. ...l1b..
0030  1f ea 07 bb 00 00 01 01  08 0a 00 01 a1 17 3b b5   ........ ......;.
```

File: "/media/8258-52FF/40DB/Re... Packets: 221098 Displayed: 1038 Marked: 0 Load time: 0:24.218 Profile: Default

DOMAIN 7 – SECURITY OPERATIONS

Understand and comply with investigations

Artifacts – Mobile Devices (Sources)

- Apple's iOS and Google's Android (mostly
- Mobile device encryption is a significant challenge.
- Cellular, WiFi, Bluetooth, and NFC are unique forensic opportunities requiring additional skill.
- Apple's Find My and Google's Find My Device allow a lost or stolen phone to be remotely locked or wiped, which destroys vital evidence.

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT LOGGING AND MONITORING ACTIVITIES

We **CANNOT** prevent all bad things from happening, so we **MUST** be able to **detect and respond**.

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT LOGGING AND MONITORING ACTIVITIES

Intrusion Detection and Prevention

- Detection detects (passive), Prevention prevents (active)
- Network-based and host-based.
- **NIDS** – network-based intrusion detection.
- **NIPS** – network-based intrusion prevention.
- **HIDS** – host-based intrusion detection.
- **HIPS** – host-based intrusion prevention.
- Best used at crucial network chokepoints, such as the **between the demilitarized zone (DMZ) and internal networks** or **between a VPN terminator and an internal network**.

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT LOGGING AND MONITORING ACTIVITIES

Intrusion Detection and Prevention

- Detection detects (passive). Prevention prevents (active)
- N
- **N**
- **N**
- **HIDS** – host-based intrusion detection.
- **HIPS** – host-based intrusion prevention.
- Best used at crucial network chokepoints, such as the **between the demilitarized zone (DMZ) and internal networks** or **between a VPN terminator and an internal network**.

False positives and false negatives must be handled carefully. Called “tuning”.

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT LOGGING AND MONITORING ACTIVITIES

Security Information and Event Management (SIEM)

- **Centralization** – centralizing log files keeps them organized and protects them.
- **Normalization** – logs from different systems come in different formats, a standardized format must be used for correlation and comparison.
- **Correlation** and **detection** – incidents often span systems, so logs/activities must be correlated for detection.
- **Alerting** – Specific events and/or incidents can be configured to alert administrators.

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT LOGGING AND MONITORING ACTIVITIES

Security Information and Event Management (SIEM)

IMPORTANT:

- Garbage in/Garbage out
- SIEM operates on rules, so the rules must be set correctly.

- **C** ized a
- **N** d or c
- **C** ns, so logs/activities must be correlated for detection.
- **Alerting** – Specific events and/or incidents can be configured to alert administrators.

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT LOGGING AND MONITORING ACTIVITIES

Continuous Monitoring

- Information Security Continuous Monitoring (ISCM).

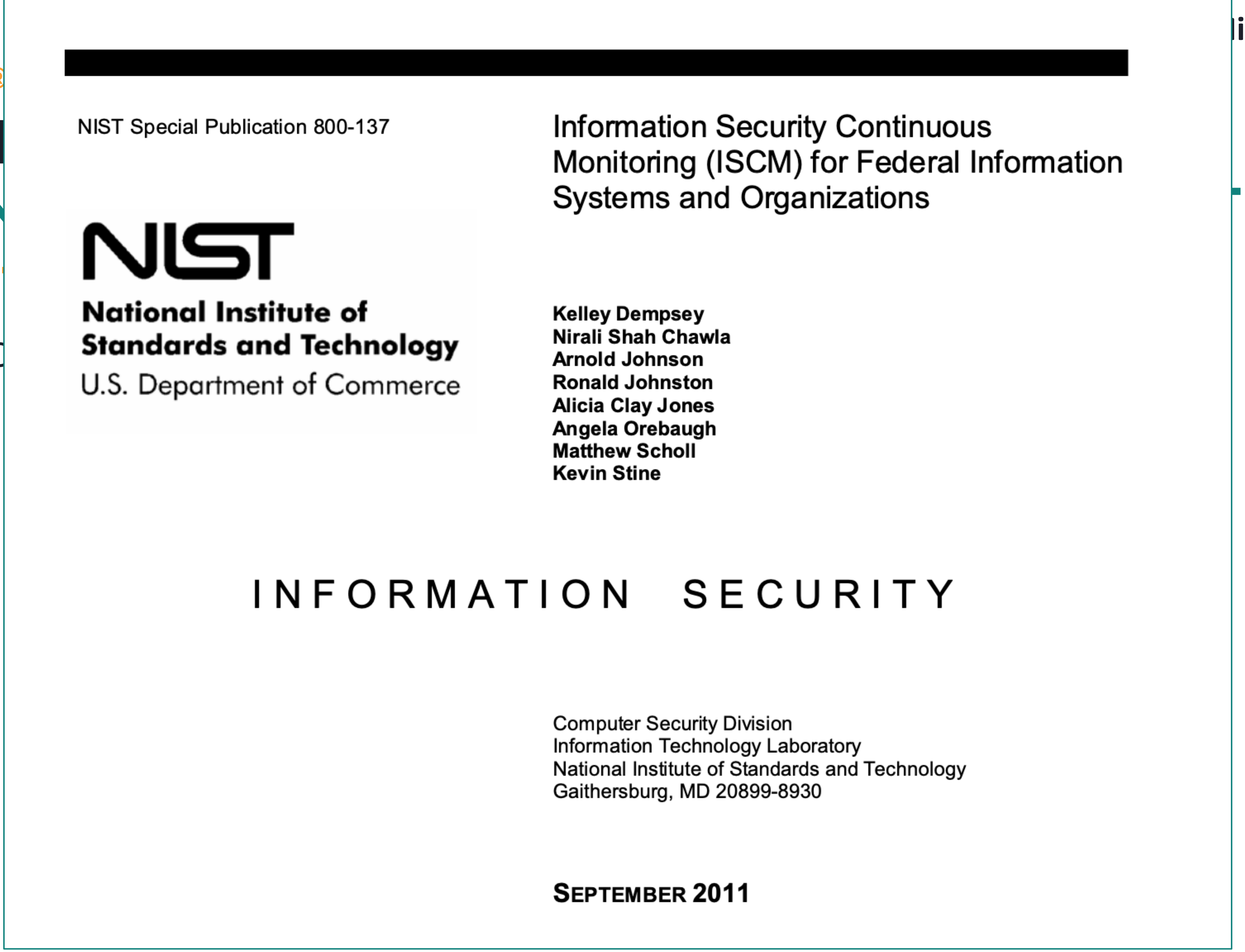
CISSP®

DO

CON TIES

Con

- Info



NIST Special Publication 800-137

Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

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

Kelley Dempsey
Nirali Shah Chawla
Arnold Johnson
Ronald Johnston
Alicia Clay Jones
Angela Orebaugh
Matthew Scholl
Kevin Stine

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

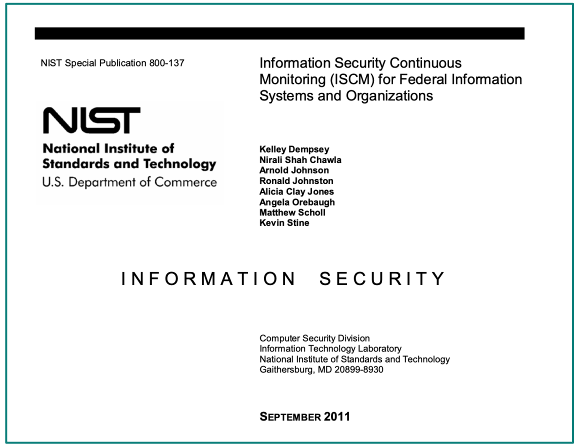
SEPTEMBER 2011

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT LOGGING AND MONITORING ACTIVITIES

Continuous Monitoring

- Information Security Continuous Monitoring (ISCM).
- Steps to establish, implement, and maintain ISCM:
  - Define an ISCM **strategy**;
  - Establish an ISCM program;
  - Implement an ISCM program;
  - Analyze data and Report findings;
  - Respond to findings; and
  - Review and Update the ISCM strategy and program.
- A robust ISCM program thus enables organizations to move from compliance-driven risk management to data-driven risk management



NIST Special Publication 800-137

Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

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

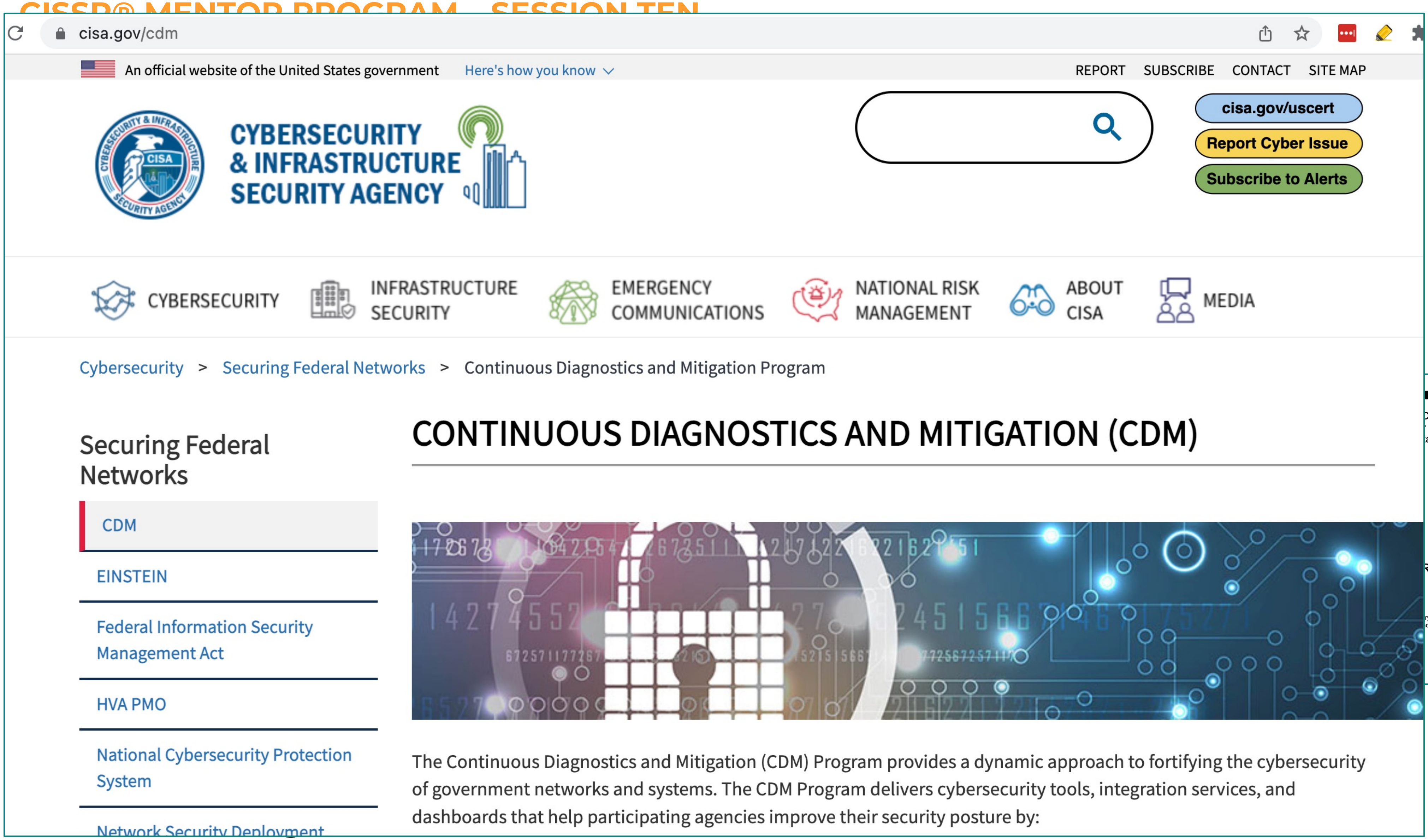
Kelley Dempsey
Nirali Shah Chawla
Arnold Johnson
Ronald Johnston
Alicia Clay Jones
Angela Orebaugh
Matthew Scholl
Kevin Stine

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

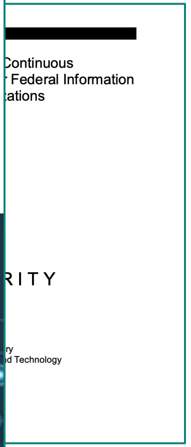
SEPTEMBER 2011

CISSP® MENTOR PROGRAM – SESSION TEN


cisa.gov/cdm
An official website of the United States government
Here's how you know
REPORT
SUBSCRIBE
CONTACT
SITE MAP
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
cisa.gov/uscert
Report Cyber Issue
Subscribe to Alerts
CYBERSECURITY
INFRASTRUCTURE SECURITY
EMERGENCY COMMUNICATIONS
NATIONAL RISK MANAGEMENT
ABOUT CISA
MEDIA
Cybersecurity > Securing Federal Networks > Continuous Diagnostics and Mitigation Program
Securing Federal Networks
CDM
EINSTEIN
Federal Information Security Management Act
HVA PMO
National Cybersecurity Protection System
Network Security Deployment

CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM)

The Continuous Diagnostics and Mitigation (CDM) Program provides a dynamic approach to fortifying the cybersecurity of government networks and systems. The CDM Program delivers cybersecurity tools, integration services, and dashboards that help participating agencies improve their security posture by:



DOMAIN 7 – SECURITY OPERATIONS

CONDUCT LOGGING AND MONITORING ACTIVITIES

Egress Monitoring

- Firewalls (and other filtering devices) should not only be configured for ingress (inbound) traffic control and monitoring, but also egress (outbound).
- This identifies potential data exfiltration and C2C traffic.
- Data Loss Prevention (DLP) is largely built on the premise of egress filtering.
- DLP can also filter/alert on specific data patterns; XXX-XX-XXXX, XXXX XXXX XXXX XXXX, etc.

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT LOGGING AND MONITORING ACTIVITIES

Log Management

- Log **strategy** is critical.
  - Why are we logging?
  - What should we be logging?
  - Where should we be logging?
  - What should trigger alerts and response?
  - Etc., Etc., Etc.
- CIS Benchmarks, DoD STIGs, manufacturer documentation, and specific standards can/should be all be leveraged.

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT LOGGING AND MONITORING ACTIVITIES

Log Management - Define Auditable Events and Thresholds

- Log settings are/should be continually tuned.
- Important events to consider logging:
  - Successful and unsuccessful **access attempts** like system logins, file or data access, and application access
  - **Changes to user permissions**, especially escalation like using sudo or other admin privileges
  - **Changes to or disabling security tools and settings** like DLP
  - Copy or export of **sensitive files**
  - **Sensitive data transactions** performed in applications

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT LOGGING AND MONITORING ACTIVITIES

Log Management - Define Auditable Events and Thresholds

- Important data to collect about the events:
  - User or process **IDs**
  - **Timestamps**, ideally in a standardized format like UTC or in a standardize time zone used by the whole organization
  - **Device identifiers**, hostname, IP address, or similar Name of object(s) accessed, like filename or function
  - **Policy identifiers** that triggered the log event, such as a failed login, admin privilege use, or file deletion

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT LOGGING AND MONITORING ACTIVITIES

Log Management - Define Auditable Events and Thresholds

- Ir

DON’T forget to protect the log data, maintain it in compliance with data retention requirements, clipping levels, etc.

C or

lame

of object(s) accessed, like filename or function

- **Policy identifiers** that triggered the log event, such as a failed login, admin privilege use, or file deletion

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT LOGGING AND MONITORING ACTIVITIES

Threat Intelligence

Wikipedia has a good definition:

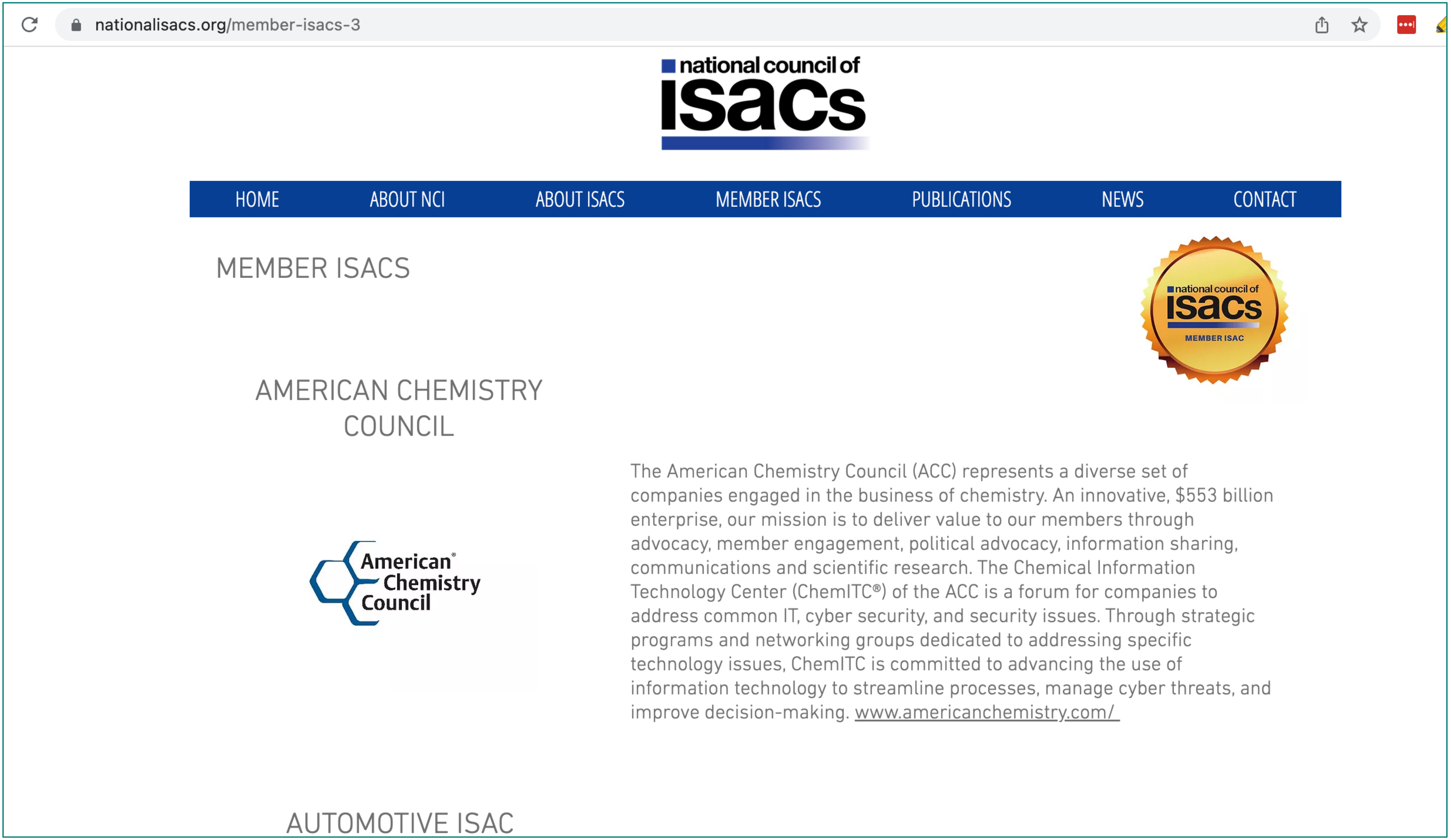
*Cyber threat intelligence (CTI) is knowledge, skills and experience-based information concerning the occurrence and assessment of both **cyber and physical threats and threat actors** that is intended to help mitigate potential attacks and harmful events occurring in cyberspace. Cyber threat intelligence **sources include open-source intelligence, social media intelligence, human Intelligence, technical intelligence, device log files, forensically acquired data or intelligence from the internet traffic and data derived for the deep and dark web**.*

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT LOGGING AND MONITORING ACTIVITIES

Threat Intelligence - Threat Feeds

- Information about threats learned about from various sources according to industry, physical region, etc.
- Data can be used for threat hunting (looking for the specific threat in an environment), integration into other tools like DLP, SIEM, and SOAR.
- Commercially available (free and paid for) threat feeds and several government-sponsored ones (mostly CISA in the United States and the Canadian Centre for Cyber Security.
- Industry-specific groups known as information sharing and analysis centers (ISACs) also offer threat information to their members.


nationalisacs.org/member-isacs-3
national council of ISACs
HOME
ABOUT NCI
ABOUT ISACS
MEMBER ISACS
PUBLICATIONS
NEWS
CONTACT
national council of ISACs MEMBER ISAC
American Chemistry Council

MEMBER ISACS

AMERICAN CHEMISTRY COUNCIL

The American Chemistry Council (ACC) represents a diverse set of companies engaged in the business of chemistry. An innovative, $553 billion enterprise, our mission is to deliver value to our members through advocacy, member engagement, political advocacy, information sharing, communications and scientific research. The Chemical Information Technology Center (ChemITC®) of the ACC is a forum for companies to address common IT, cyber security, and security issues. Through strategic programs and networking groups dedicated to addressing specific technology issues, ChemITC is committed to advancing the use of information technology to streamline processes, manage cyber threats, and improve decision-making. www.americanchemistry.com/

AUTOMOTIVE ISAC

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT LOGGING AND MONITORING ACTIVITIES

Threat Intelligence - Threat Hunting

- Seeking threats/threat actors in an environment, based upon known and unknown threats.
- Human analysts and/or software agents.
- Within an organization, can be strategic, tactical or operational.
- Outside of an organization, often done as part of security research, where a community of researchers share work and findings in the spirit of making everyone more secure.
- Details can be shared in social forums (blogs, conference talks, Twitter, etc.) and information like IoCs are integrated with security tools.

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT LOGGING AND MONITORING ACTIVITIES

Threat Intelligence - Threat Hunting

Dark Web/Deep Web

Dark web – Content on non-publicly accessible networks requiring the use of special access methods like the Tor network.

Deep web - Content accessible over the internet but not publicly exposed, such as online banking information, private social media feeds, and even content behind paywalls like news sites.

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT LOGGING AND MONITORING ACTIVITIES

User and Entity Behavior Analytics (UEBA)

Extends on an early type of cybersecurity practice – User Behavior Analytics, or UBA – which uses machine learning and deep learning to model the behavior of users on corporate networks and highlights anonymous behavior that could be the sign of a cyberattack.

Activities that deviate from expected activities (or baseline) are flagged as suspicious and can be used as an input to other security tools.

CISSP® MENTOR PROGRAM – SESSION TEN

DOMAIN 7 – SECURITY OPERATIONS

PERFORM CONFIGURATION MANAGEMENT

DOMAIN 7 – SECURITY OPERATIONS

PERFORM CONFIGURATION MANAGEMENT

Also referred to as "CM"

The Theory:

- Start with a secure configuration, make only authorized and secure changes, then the asset is maintained in a secure state.
- Items under CM are called Configuration Items (CIs).
- CIs can be systems, endpoints, applications, etc.
- The "secure configuration" of a CI is called a baseline.
- Changes to the baseline must follow a formal change management process.

CI sounds sexier than "Asset"?

CISSP® M

DOM
PERF

Also re

The Tl

- Start ɘd and secu ɹre state
- Item
- CIs c
- The '
- Char man

✓ The Two Meanings of CM

CM can be used for both configuration management and change management, which often leads to confusion as the two processes are inextricably linked but subtly different. Configuration management deals with identifying and maintaining the known good state of CIs, while change management deals with the request, approval, and implementation of changes to CIs from one secure baseline to the next.

Changes typically require the review of a change management board (CMB) or similar body, whose duty is to formally register a request for a change, assess the impact of the change, and grant approval if the proposed change does not negatively impact the security of the CI. Security practitioners should be one of the stakeholders in the CMB tasked with reviewing changes for security impact, and other stakeholders like finance and IT will also evaluate the change for cost or technology impacts.

DOMAIN 7 – SECURITY OPERATIONS

PERFORM CONFIGURATION MANAGEMENT

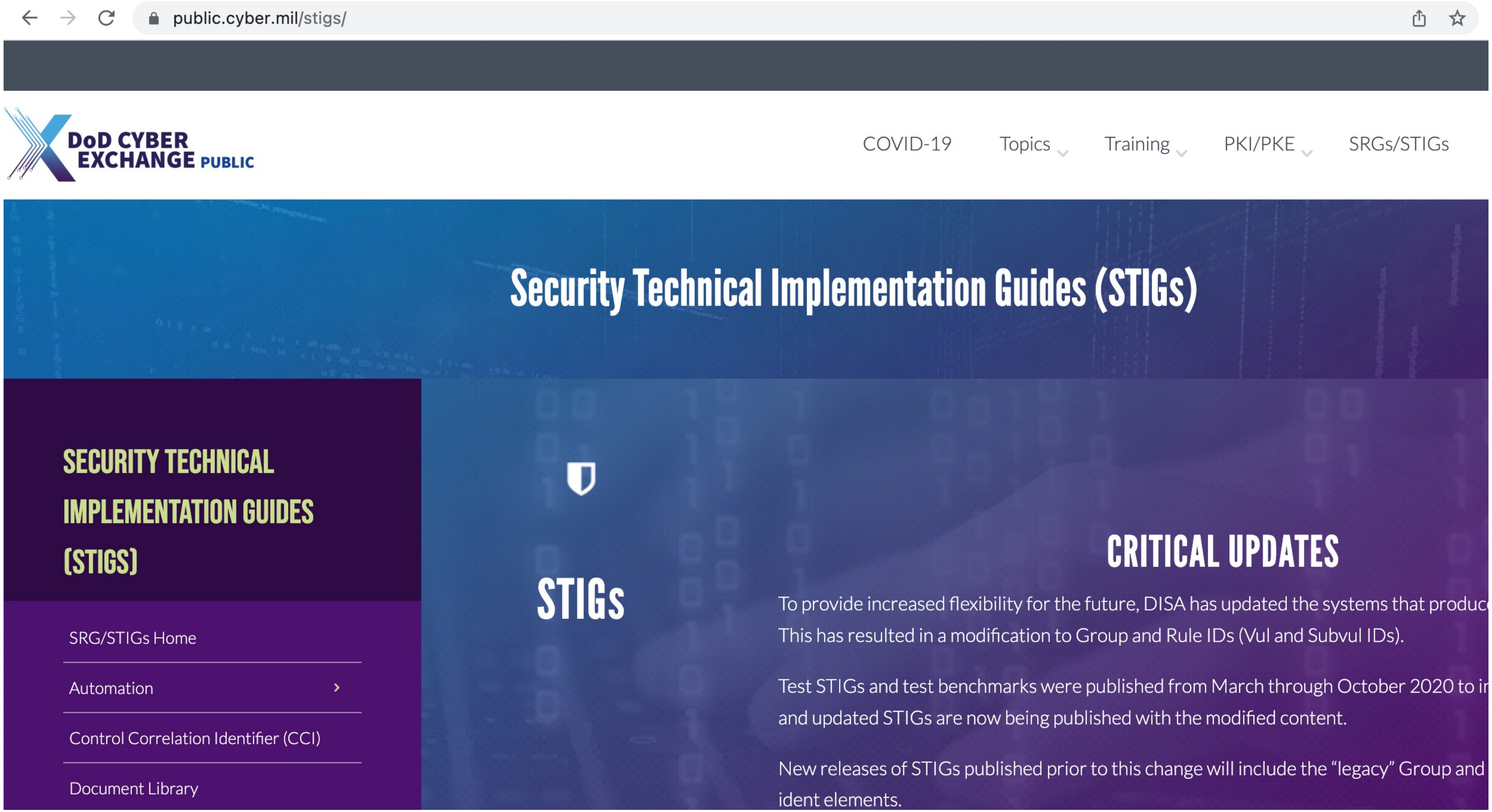
Also referred to as "CM"

Roles and responsibilities, how CM will work, etc. should be documented in a **Configuration Management Plan**.

Provisioning – setup and deployment of the secure configuration (baseline).

- The CI must be entered into the **asset inventory**.
- Baseline, standard baselines include **DISA STIGs**, **CIS Benchmarks**, and/or **vendor-supplied** configuration information.

CISSP® MENTOR PROGRAM – SESSION TEN



Security Technical Implementation Guides (STIGs)

SECURITY TECHNICAL IMPLEMENTATION GUIDES (STIGS)

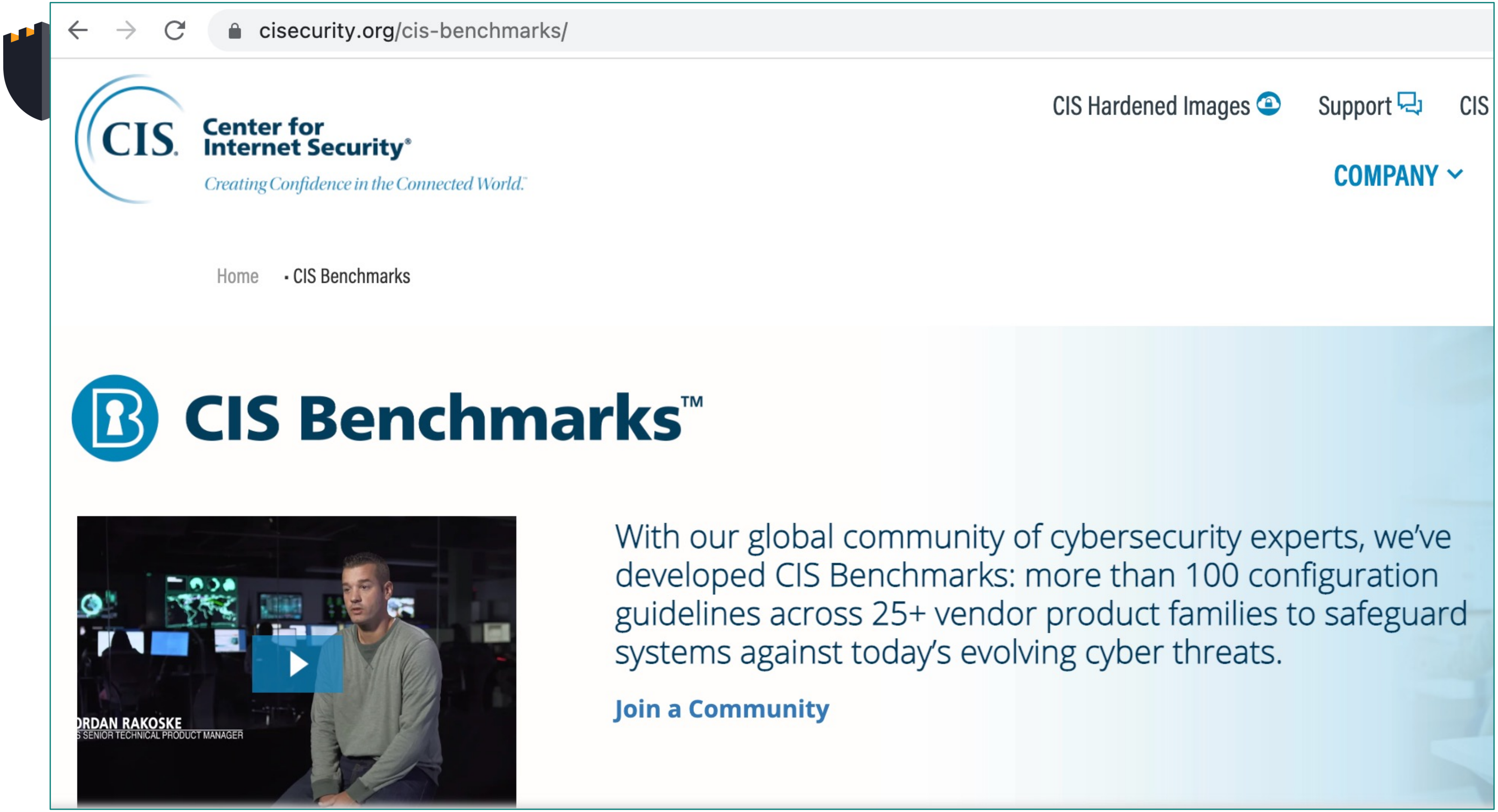
STIGs

CRITICAL UPDATES

To provide increased flexibility for the future, DISA has updated the systems that produc
This has resulted in a modification to Group and Rule IDs (Vul and Subvul IDs).

Test STIGs and test benchmarks were published from March through October 2020 to i
and updated STIGs are now being published with the modified content.

New releases of STIGs published prior to this change will include the "legacy" Group and
ident elements.



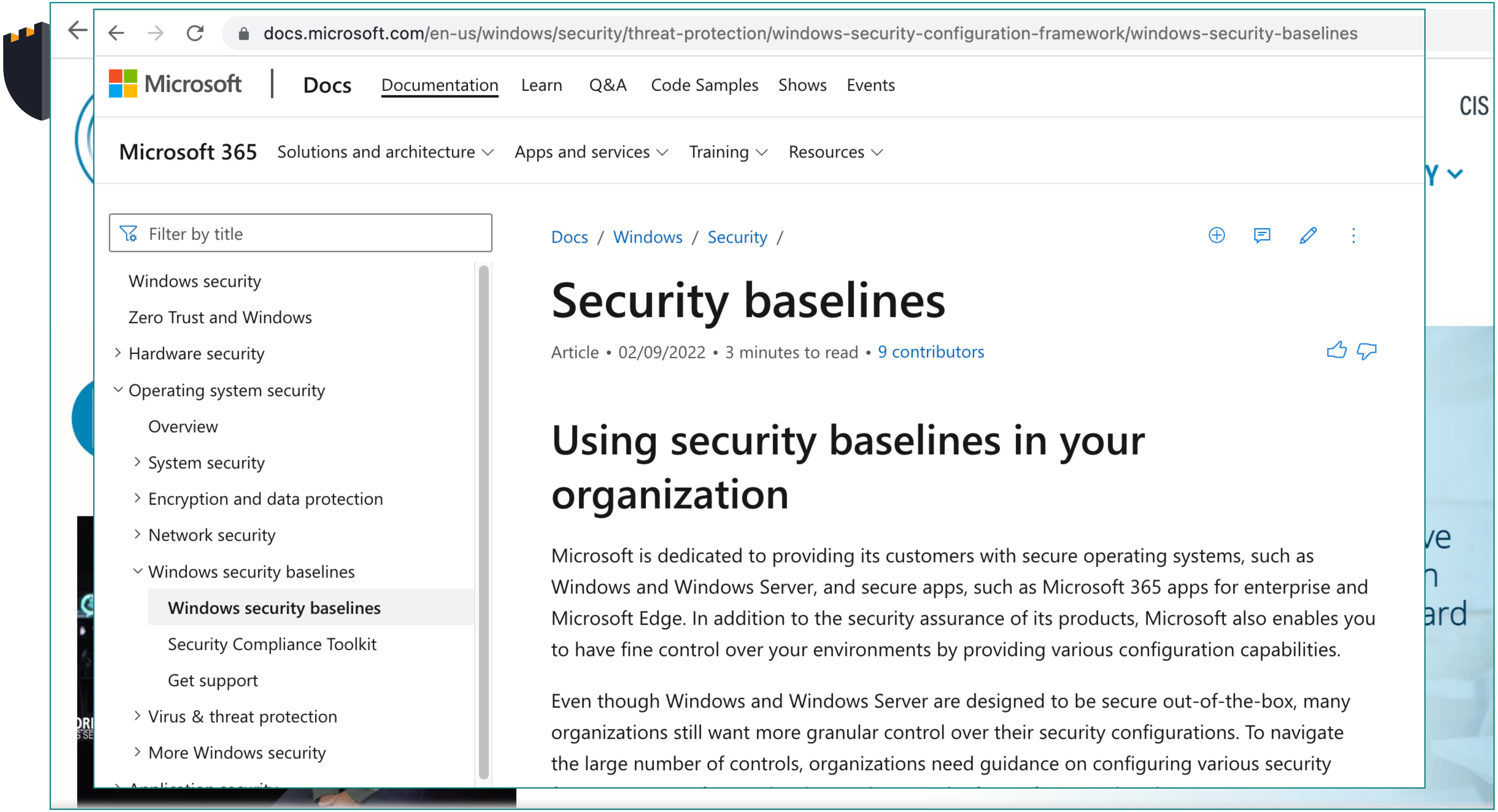
cisecurity.org/cis-benchmarks/

CIS Center for Internet Security®
Creating Confidence in the Connected World.™
CIS Hardened Images
Support
CIS
COMPANY
Home
· CIS Benchmarks
ORDAN RAKOSKE
S SENIOR TECHNICAL PRODUCT MANAGER

CIS Benchmarks™

With our global community of cybersecurity experts, we've developed CIS Benchmarks: more than 100 configuration guidelines across 25+ vendor product families to safeguard systems against today's evolving cyber threats.

Join a Community



docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines
Microsoft
Docs
Documentation
Learn
Q&A
Code Samples
Shows
Events
Microsoft 365
Solutions and architecture
Apps and services
Training
Resources
Filter by title

- Windows security
- Zero Trust and Windows
- Hardware security
- Operating system security
  - Overview
  - System security
  - Encryption and data protection
  - Network security
  - Windows security baselines
    - **Windows security baselines**
    - Security Compliance Toolkit
    - Get support
  - Virus & threat protection
  - More Windows security
- Application security

Docs / Windows / Security /

Security baselines

Article • 02/09/2022 • 3 minutes to read • 9 contributors

Using security baselines in your organization

Microsoft is dedicated to providing its customers with secure operating systems, such as Windows and Windows Server, and secure apps, such as Microsoft 365 apps for enterprise and Microsoft Edge. In addition to the security assurance of its products, Microsoft also enables you to have fine control over your environments by providing various configuration capabilities.

Even though Windows and Windows Server are designed to be secure out-of-the-box, many organizations still want more granular control over their security configurations. To navigate the large number of controls, organizations need guidance on configuring various security

DOMAIN 7 – SECURITY OPERATIONS

PERFORM CONFIGURATION MANAGEMENT

Insecure configurations are a **VERY** common cause of vulnerabilities and incidents. Use automation where possible.

Maintain the secure configuration through strict change management.

CISSP® MENTOR PROGRAM – SESSION TEN

DOMAIN 7 – SECURITY OPERATIONS

APPLY FOUNDATIONAL SECURITY OPERATIONS CONCEPTS

DOMAIN 7 – SECURITY OPERATIONS

APPLY FOUNDATIONAL SECURITY OPERATIONS CONCEPTS

Need-to-Know/Least Privilege

Need-to-know and least privilege are often used interchangeably, but they are different,

- **Need-to-know** is data-driven. Does a person/subject need to know the information? Regardless of whether the person/subject has privileges.
- **Least privilege** is system-driven. Does the person/subject need this level of access to perform an authorized job function? Also called "minimum necessary access".

DOMAIN 7 – SECURITY OPERATIONS

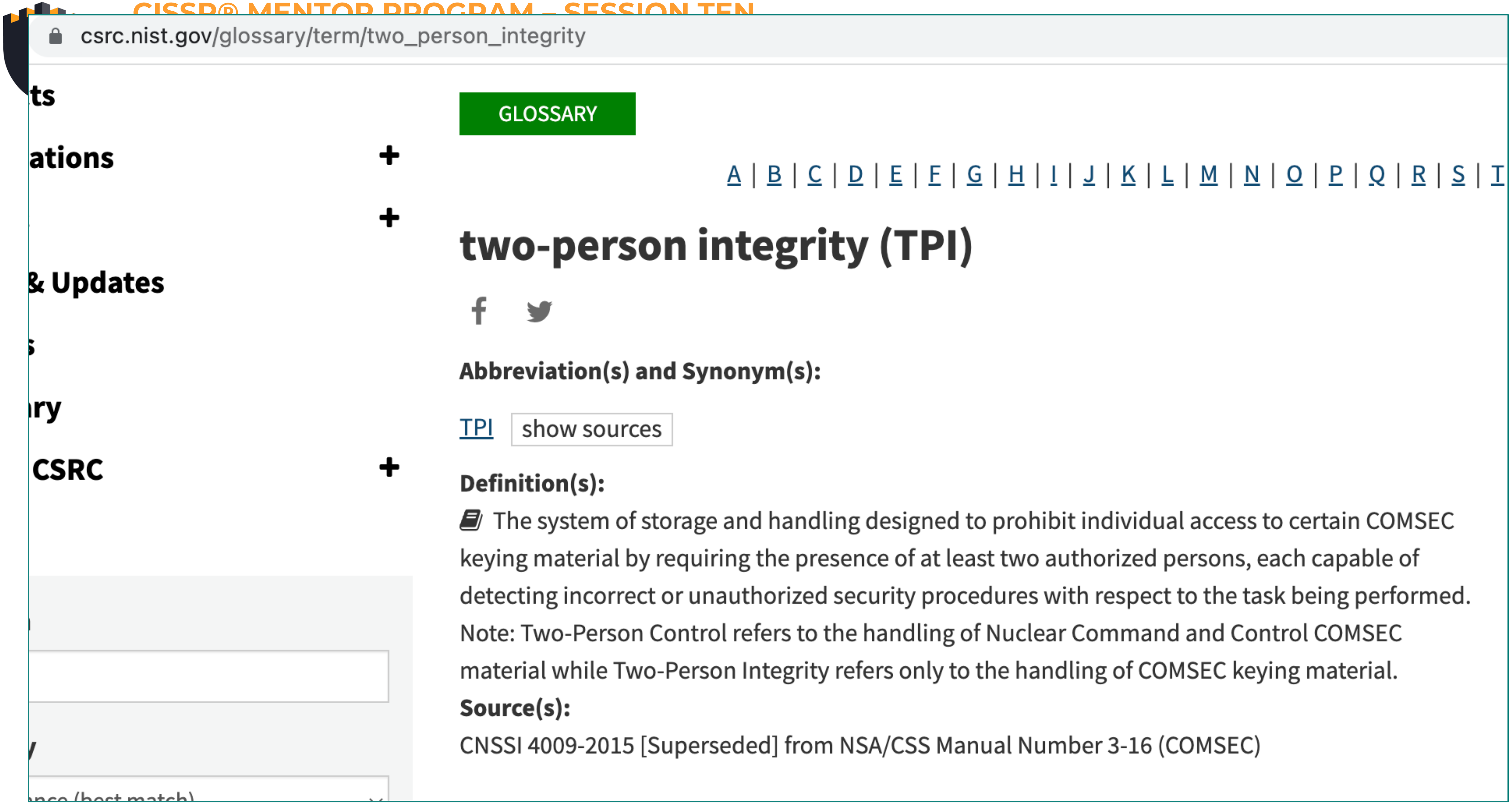
APPLY FOUNDATIONAL SECURITY OPERATIONS CONCEPTS

Separation of Duties and Responsibilities (SoD)

Limits the potential for misuse of resources or malicious activities by separating process steps among multiple personnel.

The person requesting access must not be the same one authorizing access and/or granting access.

- **Dual control** - A process that uses two or more separate entities (usually persons) operating in concert to protect sensitive functions or information.
- **Two-person integrity** - no single person can access an asset like a file or piece of equipment without another authorized individual present.



csrc.nist.gov/glossary/term/two_person_integrity
ts
ations +
+
& Updates
ry
CSRC +
nce (best match)
GLOSSARY
A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T

two-person integrity (TPI)

Abbreviation(s) and Synonym(s):

TPI show sources

Definition(s):

The system of storage and handling designed to prohibit individual access to certain COMSEC keying material by requiring the presence of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed. Note: Two-Person Control refers to the handling of Nuclear Command and Control COMSEC material while Two-Person Integrity refers only to the handling of COMSEC keying material.

Source(s):

CNSSI 4009-2015 [Superseded] from NSA/CSS Manual Number 3-16 (COMSEC)

DOMAIN 7 – SECURITY OPERATIONS

APPLY FOUNDATIONAL SECURITY OPERATIONS CONCEPTS

Privileged Account Management (PAM)

- Privileges, often called permissions, are the abilities a user is granted on a system.
- Privileged accounts (those with “elevate” privileges) require additional rigor during the access management lifecycle, such as more frequent reviews, MFA, limited use, etc..
- Provisioning, Use, Review, and Deprovisioning requirements must all be considered.

DOMAIN 7 – SECURITY OPERATIONS

APPLY FOUNDATIONAL SECURITY OPERATIONS CONCEPTS

Job Rotation

- **Two primary benefits**
  - Cross-training which improves operational resilience.
  - Limits/mitigates internal fraud (and related)
    - Personnel are less-likely to engage when they know they rotate and
    - Fraud is more likely to be detected.

DOMAIN 7 – SECURITY OPERATIONS

APPLY FOUNDATIONAL SECURITY OPERATIONS CONCEPTS

Service-Level Agreements

- Defines the level of service expected from a third party:
  - The metrics by which service is measured,
  - Remedies or penalties should agreed-on service levels not be achieved
- It is a critical component of any technology vendor contract.
- A mutual agreement of service level requirements (SLRs) is an SLA, which codifies the shared understanding of SLRs.
- SLAs should be monitored continually and should be part of third-party information security risk management.

CISSP® MENTOR PROGRAM – SESSION TEN

DOMAIN 7 – SECURITY OPERATIONS

APPLY RESOURCE PROTECTION

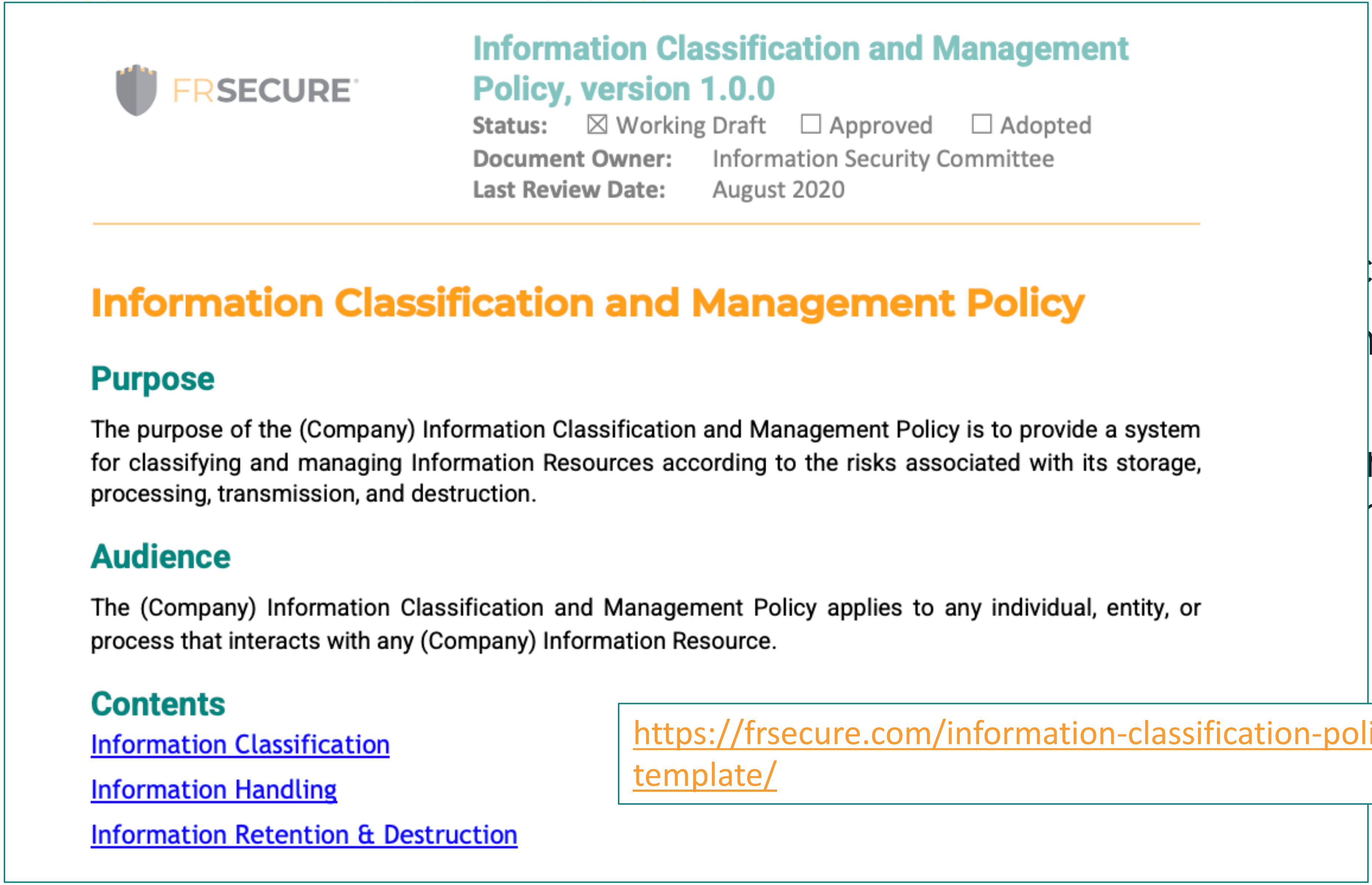
DOMAIN 7 – SECURITY OPERATIONS

APPLY RESOURCE PROTECTION

Media Management

- Physical and electronic; paper, hard drives, devices, etc.
- ALL data should be classified as part of data management practices.
- **Labeling and Marking** is driven from data classification requirements, using the highest classification on the media.

CISSP® MENTOR PROGRAM – SESSION TEN



FRSECURE

Information Classification and Management Policy, version 1.0.0

Status: ☒ Working Draft ☐ Approved ☐ Adopted

Document Owner: Information Security Committee

Last Review Date: August 2020

Information Classification and Management Policy

Purpose

The purpose of the (Company) Information Classification and Management Policy is to provide a system for classifying and managing Information Resources according to the risks associated with its storage, processing, transmission, and destruction.

Audience

The (Company) Information Classification and Management Policy applies to any individual, entity, or process that interacts with any (Company) Information Resource.

Contents

Information Classification

Information Handling

Information Retention & Destruction

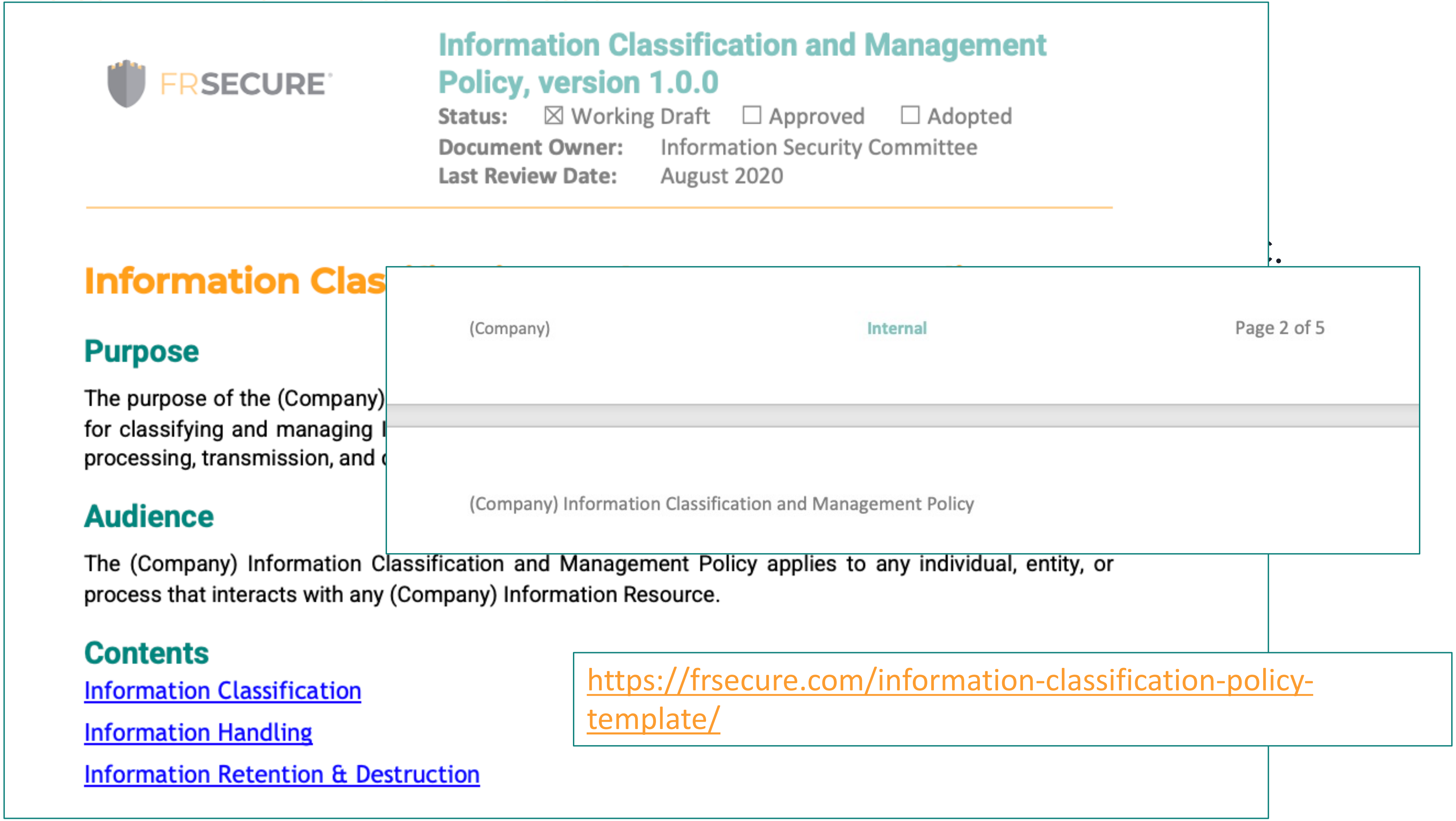
:.

ent

n

edia.

https://frsecure.com/information-classification-policy-template/



FRSECURE

Information Classification and Management Policy, version 1.0.0

Status: ☒ Working Draft ☐ Approved ☐ Adopted

Document Owner: Information Security Committee

Last Review Date: August 2020

Information Clas

Purpose

The purpose of the (Company)
for classifying and managing I
processing, transmission, and (

Audience

The (Company) Information Classification and Management Policy applies to any individual, entity, or process that interacts with any (Company) Information Resource.

Contents

- Information Classification
- Information Handling
- Information Retention & Destruction

(Company) Internal Page 2 of 5

(Company) Information Classification and Management Policy

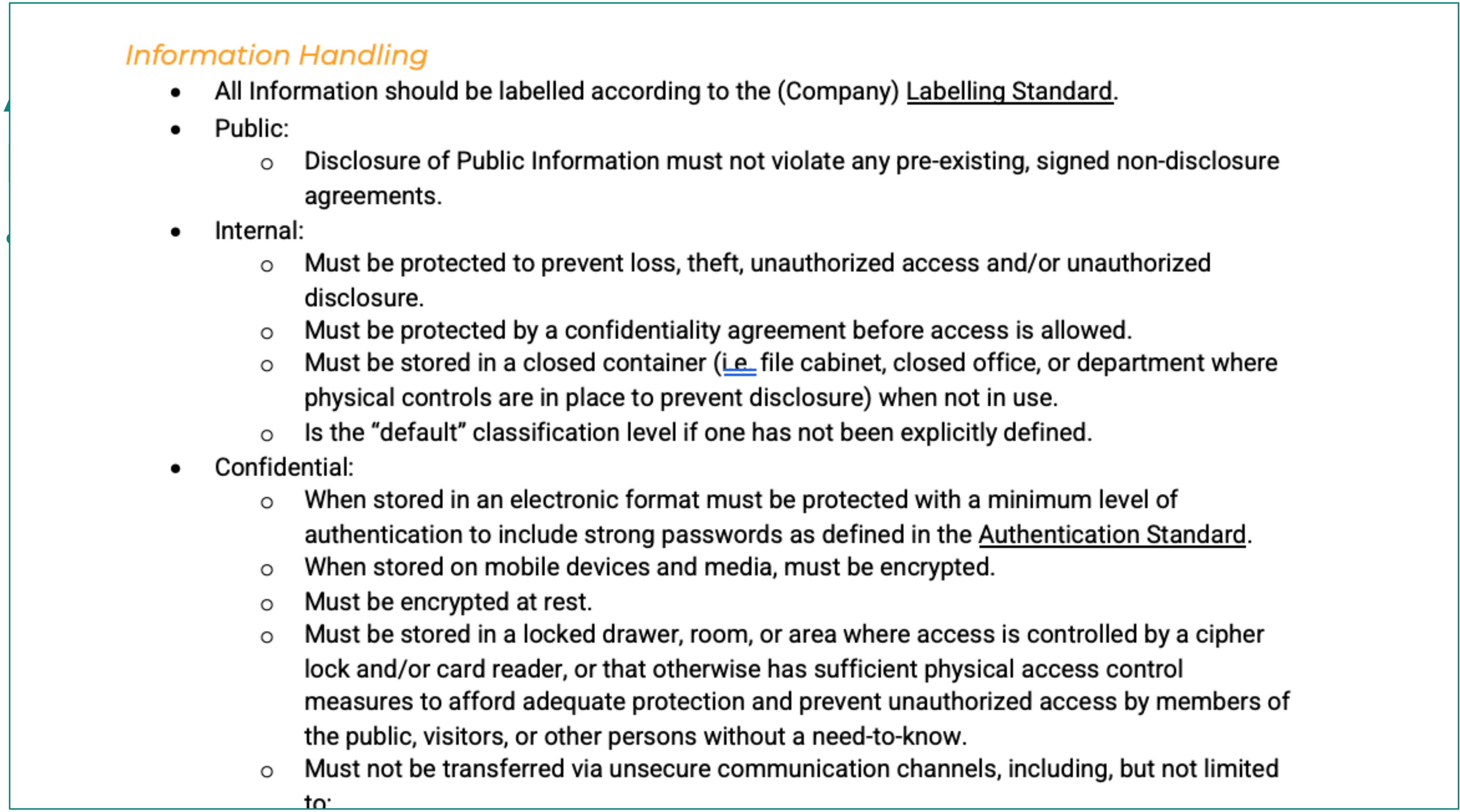
https://frsecure.com/information-classification-policy-template/

DOMAIN 7 – SECURITY OPERATIONS

APPLY RESOURCE PROTECTION

Handling

- The labeling and marking communicates to the asset holder what the protection requirements are (based upon the classification).



Information Handling

- All Information should be labelled according to the (Company) Labelling Standard.
- Public:
    - Disclosure of Public Information must not violate any pre-existing, signed non-disclosure agreements.
- Internal:
    - Must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure.
    - Must be protected by a confidentiality agreement before access is allowed.
    - Must be stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.
    - Is the “default” classification level if one has not been explicitly defined.
- Confidential:
    - When stored in an electronic format must be protected with a minimum level of authentication to include strong passwords as defined in the Authentication Standard.
    - When stored on mobile devices and media, must be encrypted.
    - Must be encrypted at rest.
    - Must be stored in a locked drawer, room, or area where access is controlled by a cipher lock and/or card reader, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.
    - Must not be transferred via unsecure communication channels, including, but not limited to:

DOMAIN 7 – SECURITY OPERATIONS

APPLY RESOURCE PROTECTION

Media Protection Techniques

Physical compromise is total compromise. RoT

Transporting Media

Encryption, hashing, and physical protections should all be considered. Physical protections should also include environmental controls.

Sanitization and Disposal

- Previously covered. Full disk encryption (FDE) is a mitigating control.
- Data must be securely overwritten and/or destroyed.

CISSP® MENTOR PROGRAM – SESSION TEN

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT INCIDENT MANAGEMENT

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT INCIDENT MANAGEMENT

First, you MUST define what an “incident” is.

An **event** is something that happened.

An **incident** is ~~something that happened~~ an event with a negative consequence.

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT INCIDENT MANAGEMENT

Incident Management Plan

Contains how the organization will manage an incident from beginning to end (and into the next).

The book, “tools, resources, and processes needed to identify, categorize, and remediate the impact of incidents.”

Plenty of standards to draw from:

- ITIL framework incident management processes
- NIST Special Publication 800-61, “Computer Security Incident Handling Guide”
- ISO 27035, “Security incident management”
- European Network and Information Security Agency (ENISA), “CSIRT Setting Up Guide”
- ISACA, “Incident Management and Response”

CISSP® MENTOR PROGRAM – SESSION TEN

DOM

CONI

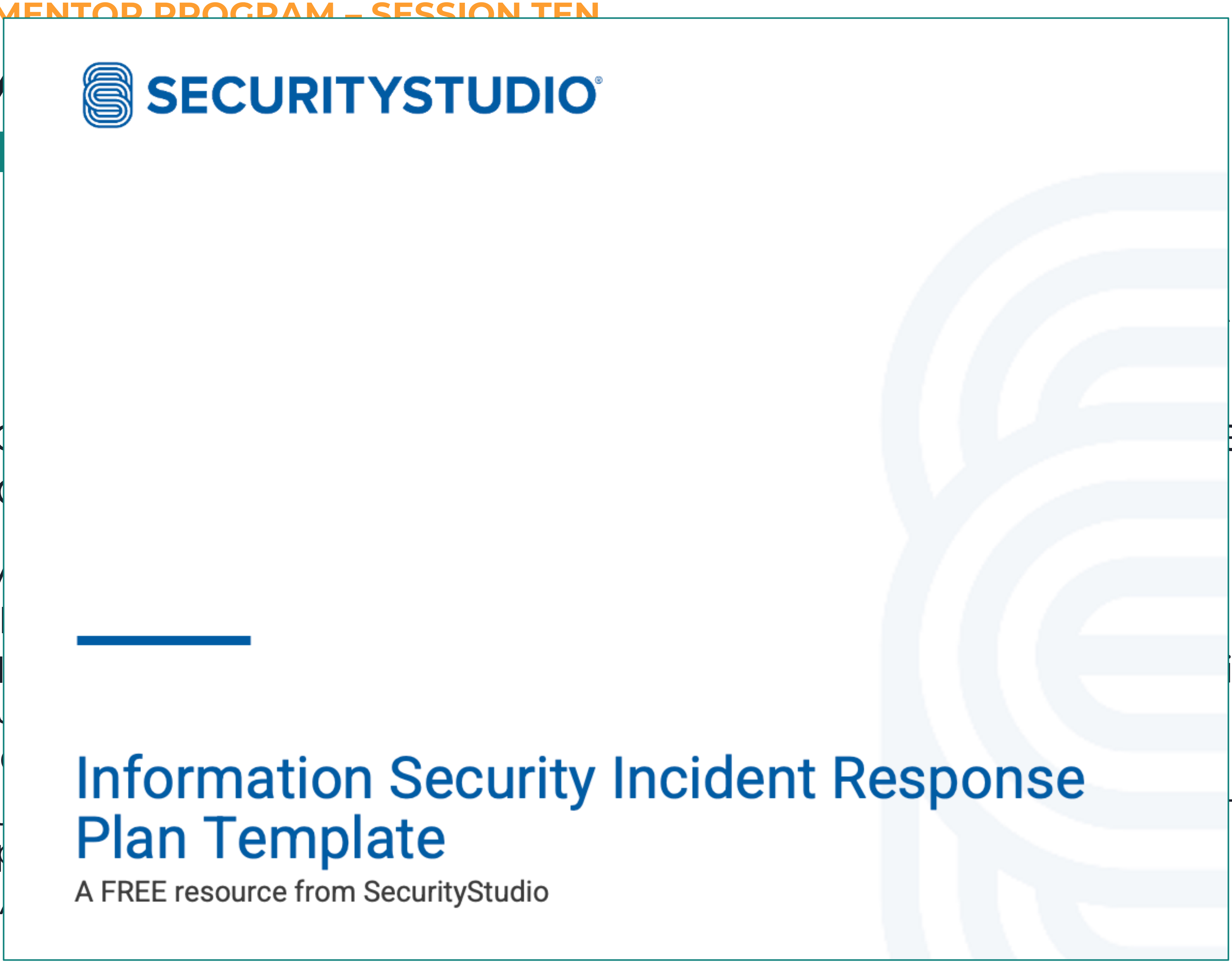
Incid

Conta from
begin

The bo entify,
catego

Plenty

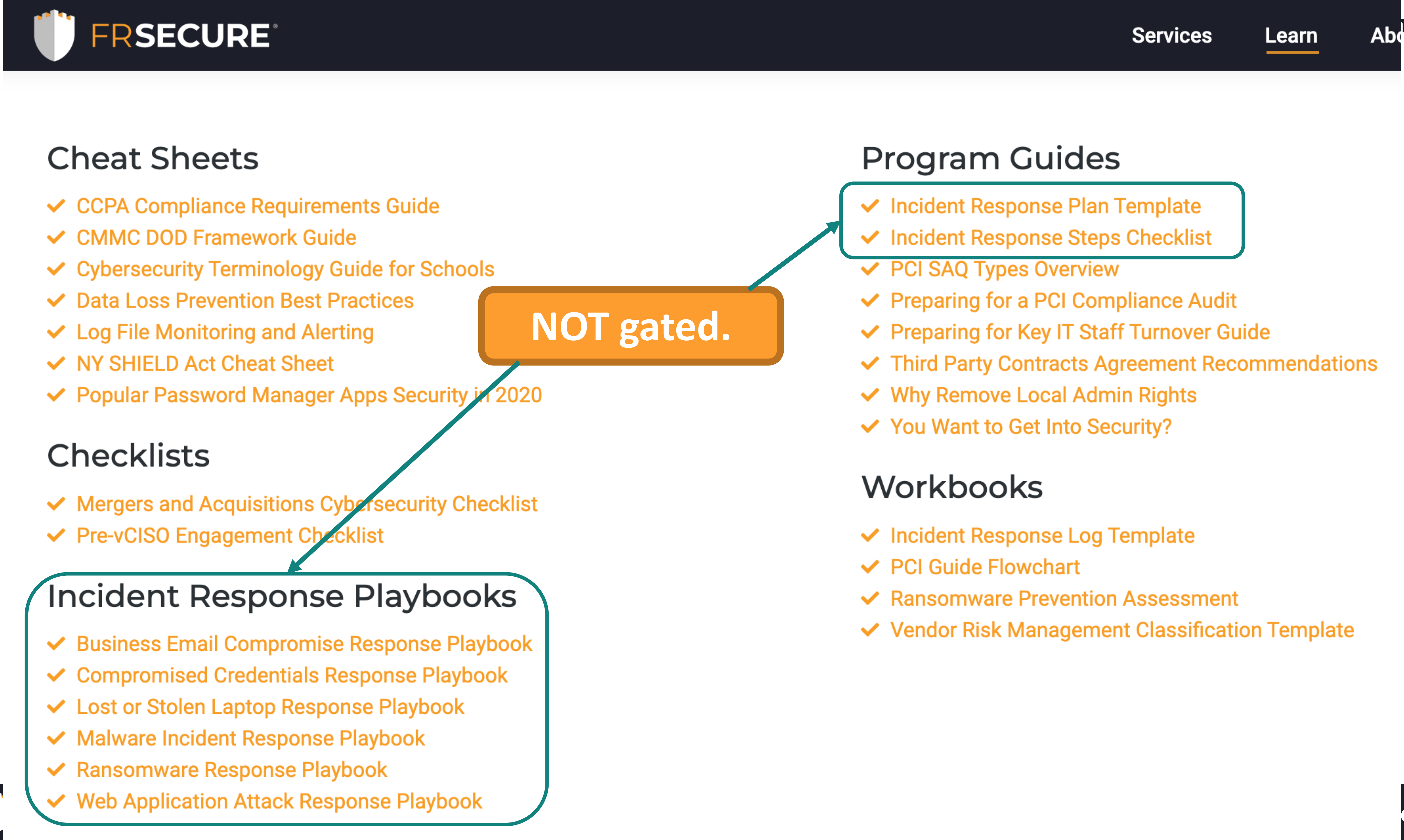
- ITI
- NI ing
  Gu
- IS
- Eu Setting
  Up
- IS



SECURITYSTUDIO®

Information Security Incident Response Plan Template

A FREE resource from SecurityStudio



NOT gated.

Cheat Sheets

- ✓ CCPA Compliance Requirements Guide
- ✓ CMMC DOD Framework Guide
- ✓ Cybersecurity Terminology Guide for Schools
- ✓ Data Loss Prevention Best Practices
- ✓ Log File Monitoring and Alerting
- ✓ NY SHIELD Act Cheat Sheet
- ✓ Popular Password Manager Apps Security in 2020

Checklists

- ✓ Mergers and Acquisitions Cybersecurity Checklist
- ✓ Pre-vCISO Engagement Checklist

Incident Response Playbooks

- ✓ Business Email Compromise Response Playbook
- ✓ Compromised Credentials Response Playbook
- ✓ Lost or Stolen Laptop Response Playbook
- ✓ Malware Incident Response Playbook
- ✓ Ransomware Response Playbook
- ✓ Web Application Attack Response Playbook

Program Guides

- ✓ Incident Response Plan Template
- ✓ Incident Response Steps Checklist
- ✓ PCI SAQ Types Overview
- ✓ Preparing for a PCI Compliance Audit
- ✓ Preparing for Key IT Staff Turnover Guide
- ✓ Third Party Contracts Agreement Recommendations
- ✓ Why Remove Local Admin Rights
- ✓ You Want to Get Into Security?

Workbooks

- ✓ Incident Response Log Template
- ✓ PCI Guide Flowchart
- ✓ Ransomware Prevention Assessment
- ✓ Vendor Risk Management Classification Template

CISSP® MENTOR PROGRAM – SESSION TEN

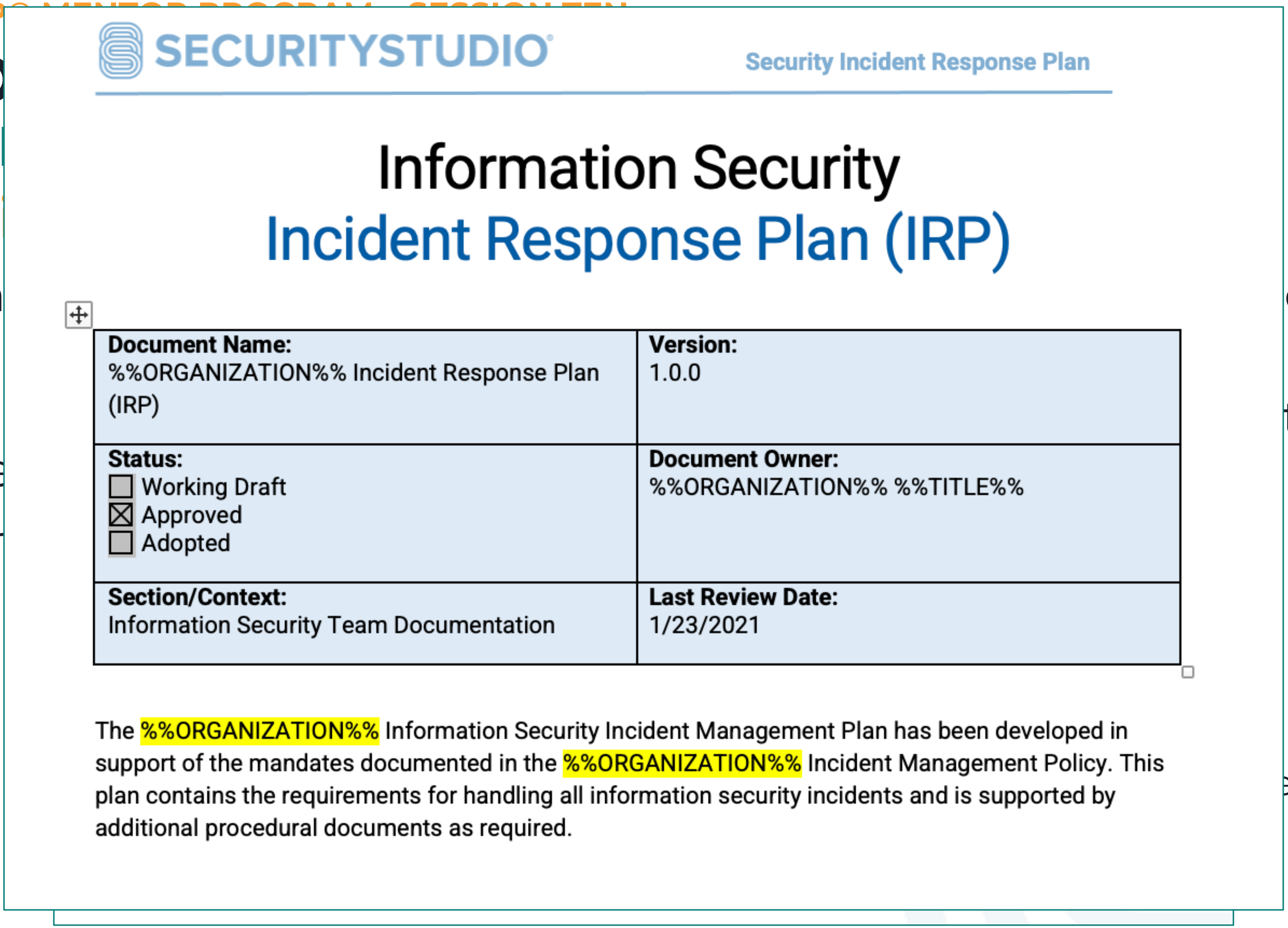
DO
CO
Inci

Con om
beg

The tify,
cate

Plen

-
-
-
- etting
-



SECURITYSTUDIO®

Security Incident Response Plan

Information Security
Incident Response Plan (IRP)

Document Name: %%ORGANIZATION%% Incident Response Plan (IRP)	**Version:** 1.0.0
Status: ☐ Working Draft ☒ Approved ☐ Adopted	**Document Owner:** %%ORGANIZATION%% %%TITLE%%
Section/Context: Information Security Team Documentation	**Last Review Date:** 1/23/2021

The %%ORGANIZATION%% Information Security Incident Management Plan has been developed in support of the mandates documented in the %%ORGANIZATION%% Incident Management Policy. This plan contains the requirements for handling all information security incidents and is supported by additional procedural documents as required.

CISSP

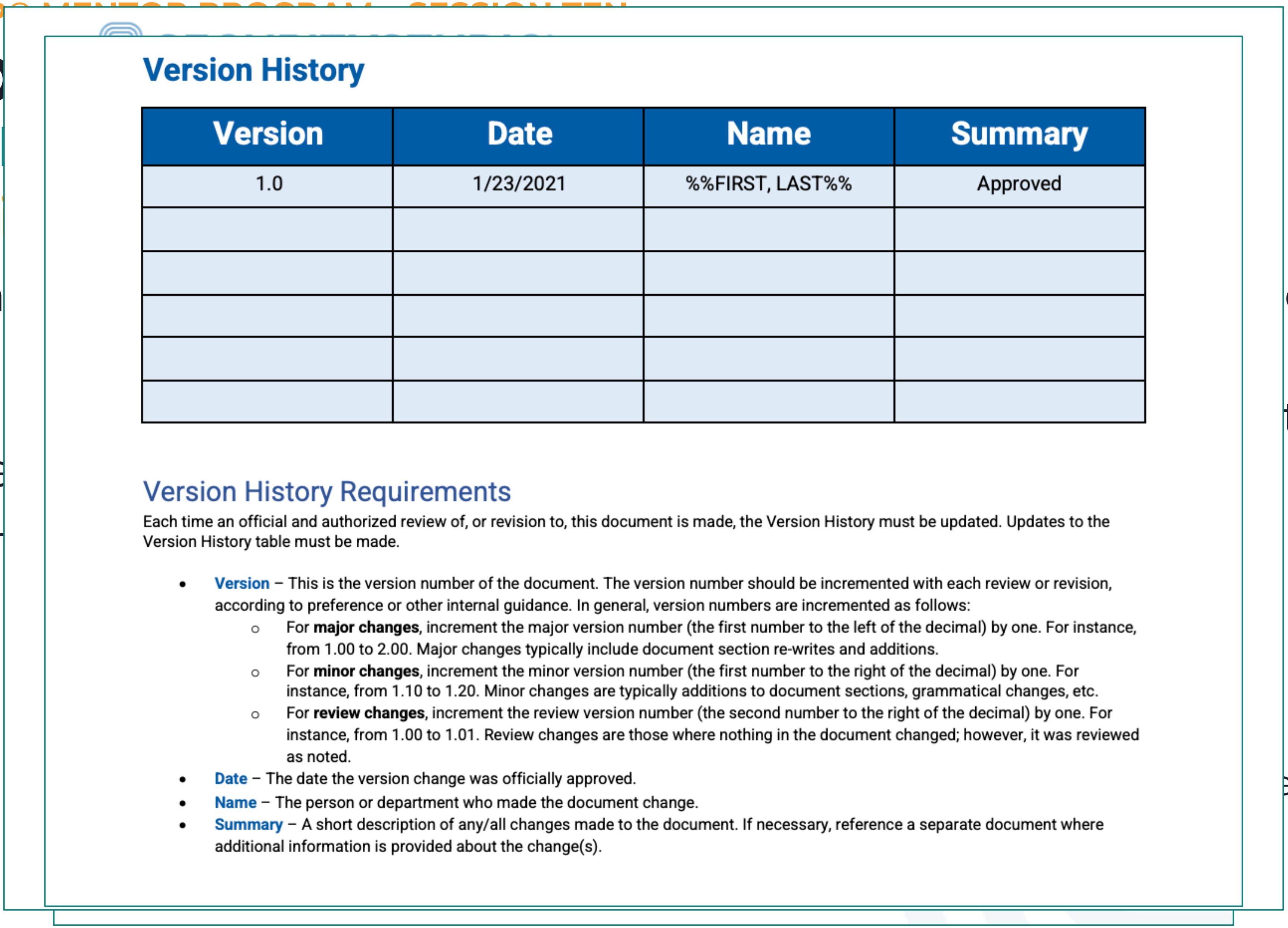
DO
CO
Inci

Con ... om
beg

The ... tify,
cate

Plen

... etting



Version History

Version	Date	Name	Summary
1.0	1/23/2021	%%FIRST, LAST%%	Approved

Version History Requirements

Each time an official and authorized review of, or revision to, this document is made, the Version History must be updated. Updates to the Version History table must be made.

- **Version** – This is the version number of the document. The version number should be incremented with each review or revision, according to preference or other internal guidance. In general, version numbers are incremented as follows:
  - For **major changes**, increment the major version number (the first number to the left of the decimal) by one. For instance, from 1.00 to 2.00. Major changes typically include document section re-writes and additions.
  - For **minor changes**, increment the minor version number (the first number to the right of the decimal) by one. For instance, from 1.10 to 1.20. Minor changes are typically additions to document sections, grammatical changes, etc.
  - For **review changes**, increment the review version number (the second number to the right of the decimal) by one. For instance, from 1.00 to 1.01. Review changes are those where nothing in the document changed; however, it was reviewed as noted.
- **Date** – The date the version change was officially approved.
- **Name** – The person or department who made the document change.
- **Summary** – A short description of any/all changes made to the document. If necessary, reference a separate document where additional information is provided about the change(s).

CI

D

C

Ir

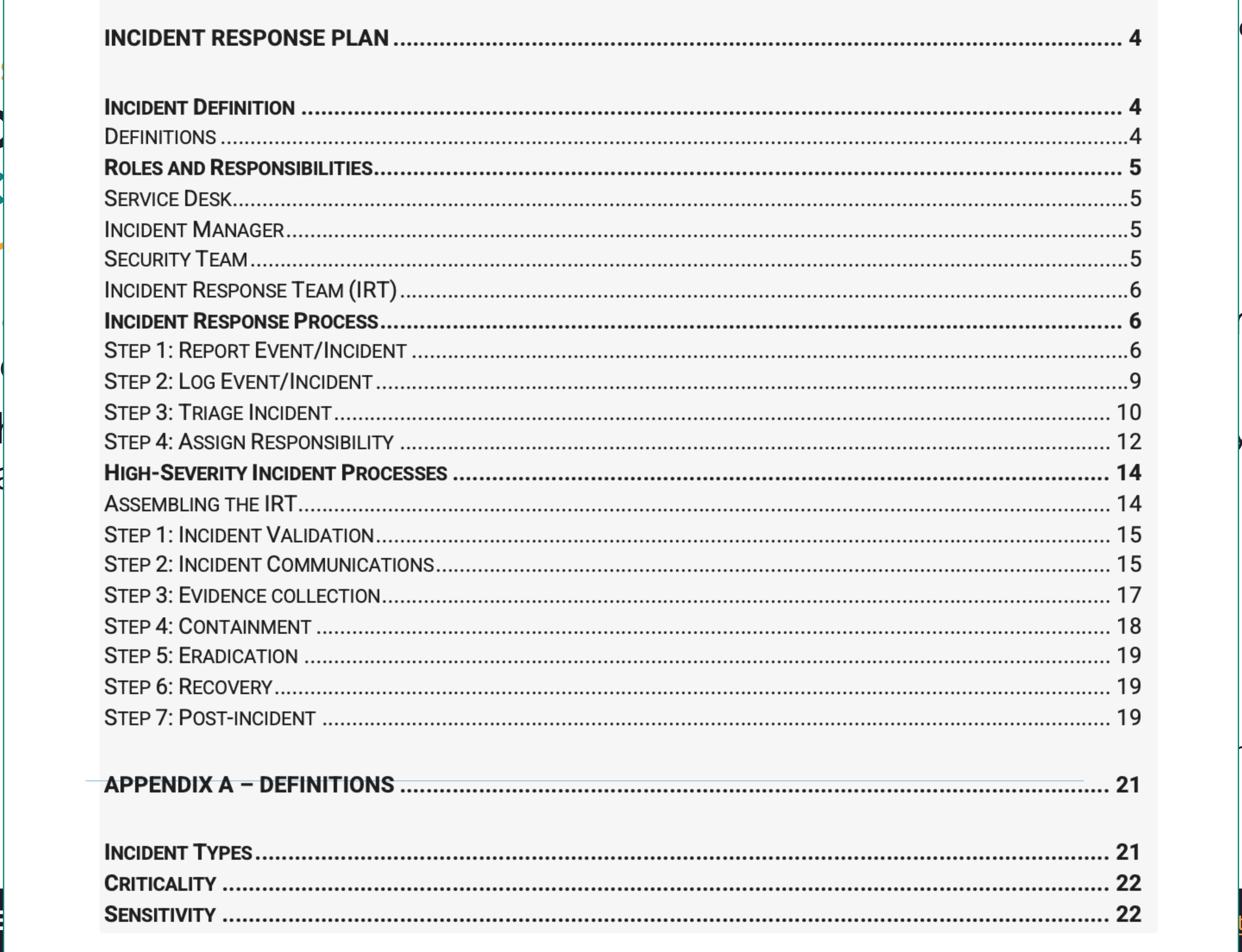
C

b

Th

ca

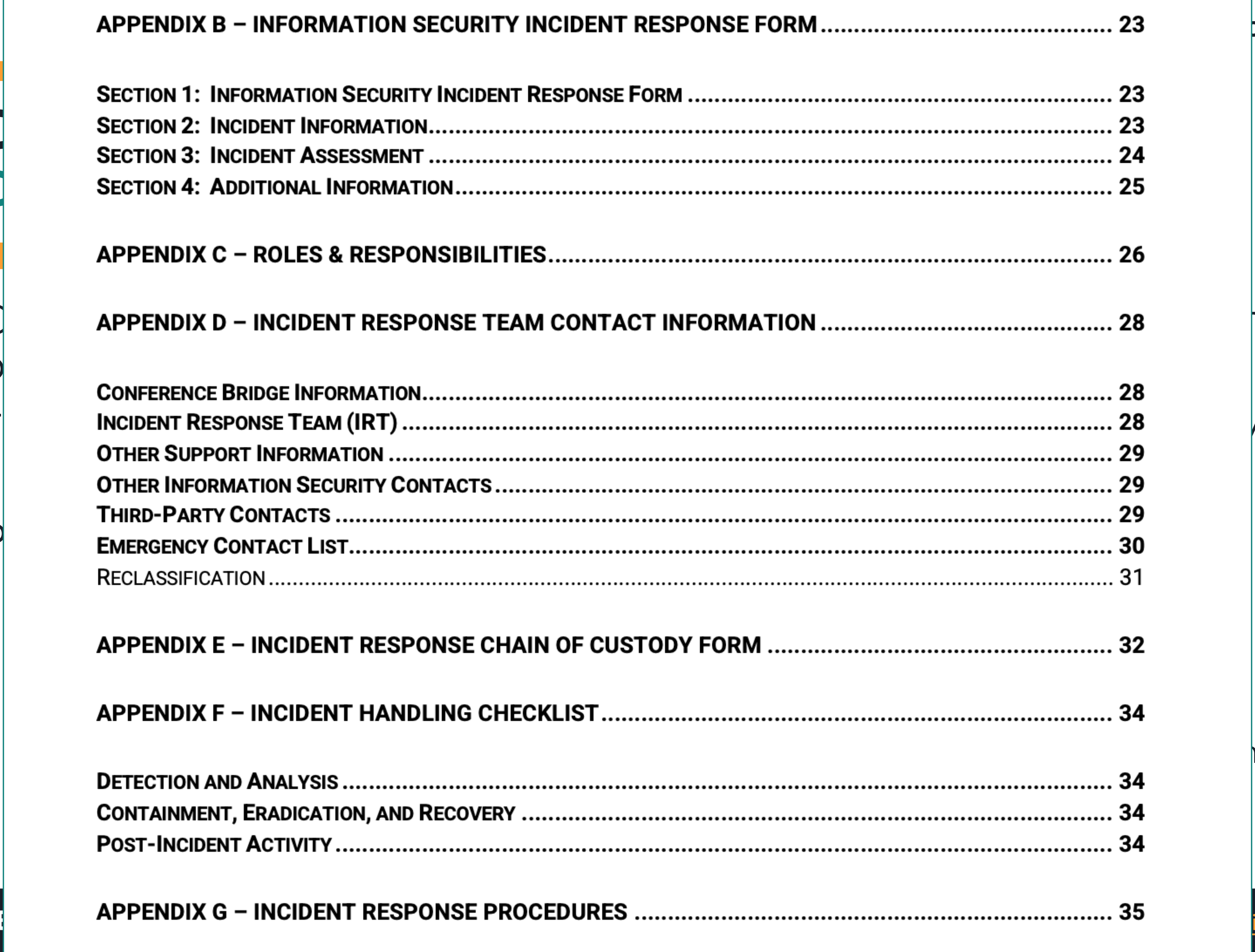
P

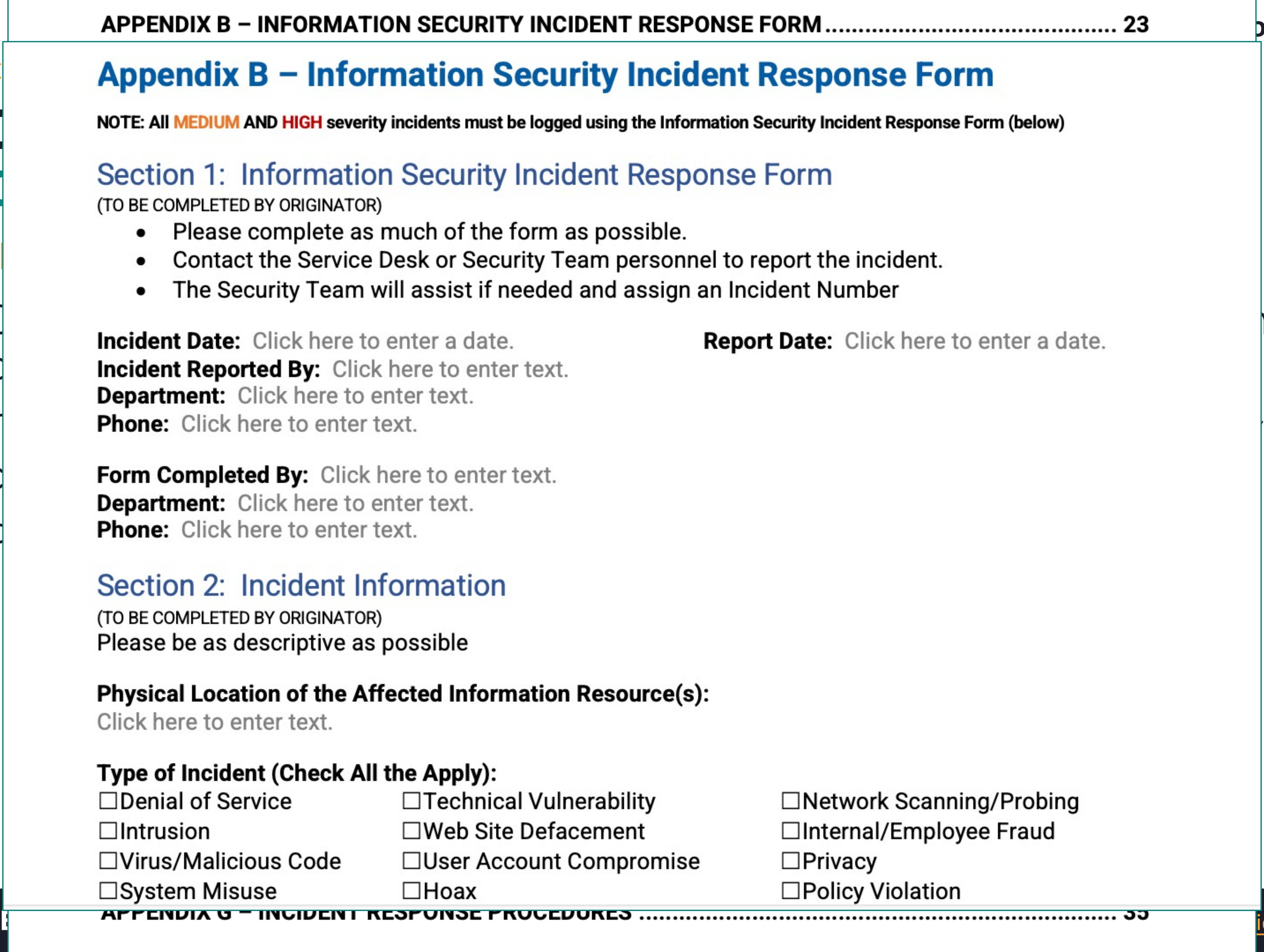


n

y,

ng





Appendix B – Information Security Incident Response Form

NOTE: All MEDIUM AND HIGH severity incidents must be logged using the Information Security Incident Response Form (below)

Section 1: Information Security Incident Response Form

(TO BE COMPLETED BY ORIGINATOR)

- Please complete as much of the form as possible.
- Contact the Service Desk or Security Team personnel to report the incident.
- The Security Team will assist if needed and assign an Incident Number

Incident Date: Click here to enter a date. **Report Date:** Click here to enter a date.
Incident Reported By: Click here to enter text.
Department: Click here to enter text.
Phone: Click here to enter text.

Form Completed By: Click here to enter text.
Department: Click here to enter text.
Phone: Click here to enter text.

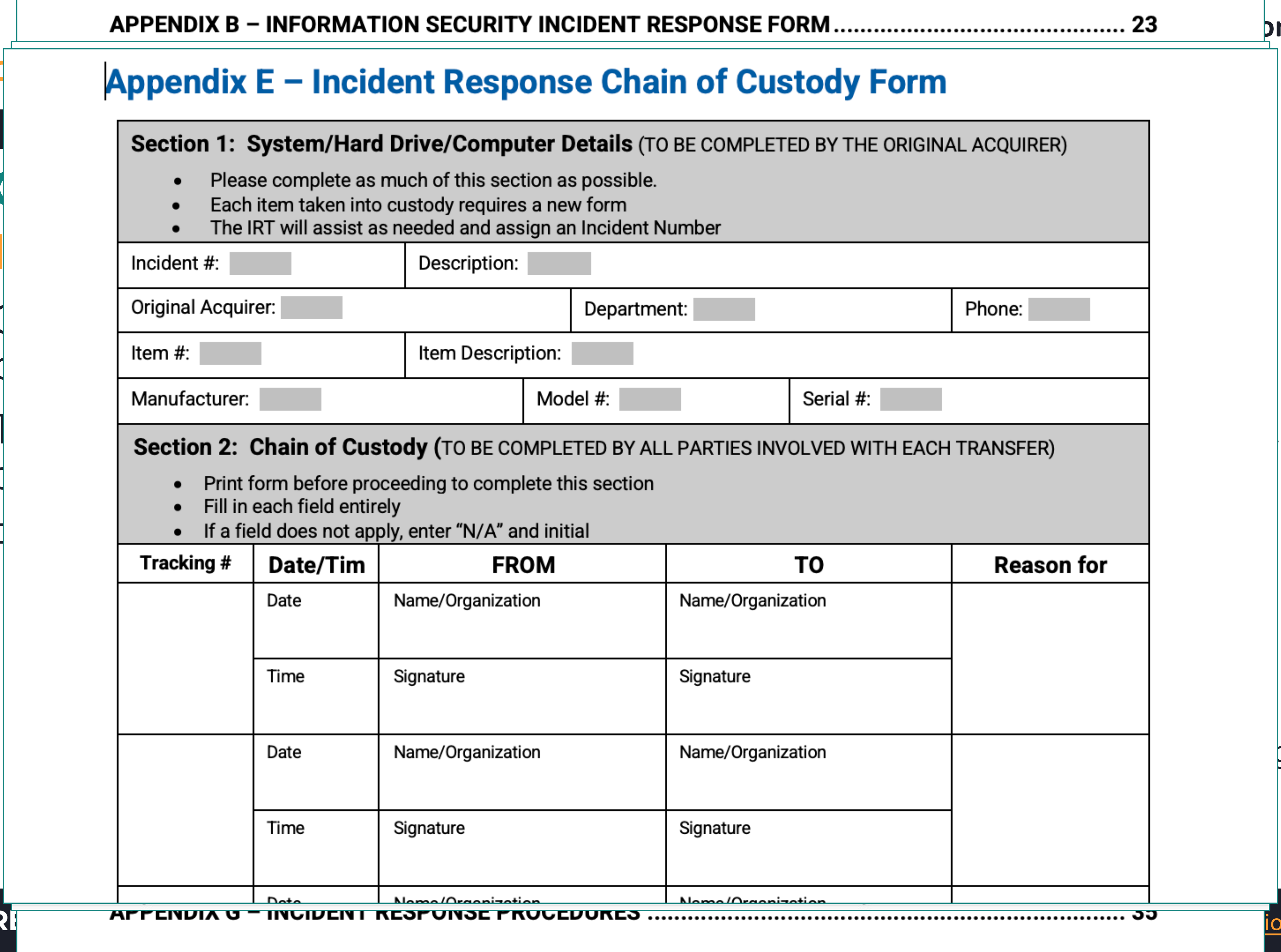
Section 2: Incident Information

(TO BE COMPLETED BY ORIGINATOR)
Please be as descriptive as possible

Physical Location of the Affected Information Resource(s):
Click here to enter text.

Type of Incident (Check All the Apply):

☐Denial of Service
☐Intrusion
☐Virus/Malicious Code
☐System Misuse
☐Technical Vulnerability
☐Web Site Defacement
☐User Account Compromise
☐Hoax
☐Network Scanning/Probing
☐Internal/Employee Fraud
☐Privacy
☐Policy Violation



Appendix E – Incident Response Chain of Custody Form

Section 1: System/Hard Drive/Computer Details (TO BE COMPLETED BY THE ORIGINAL ACQUIRER)

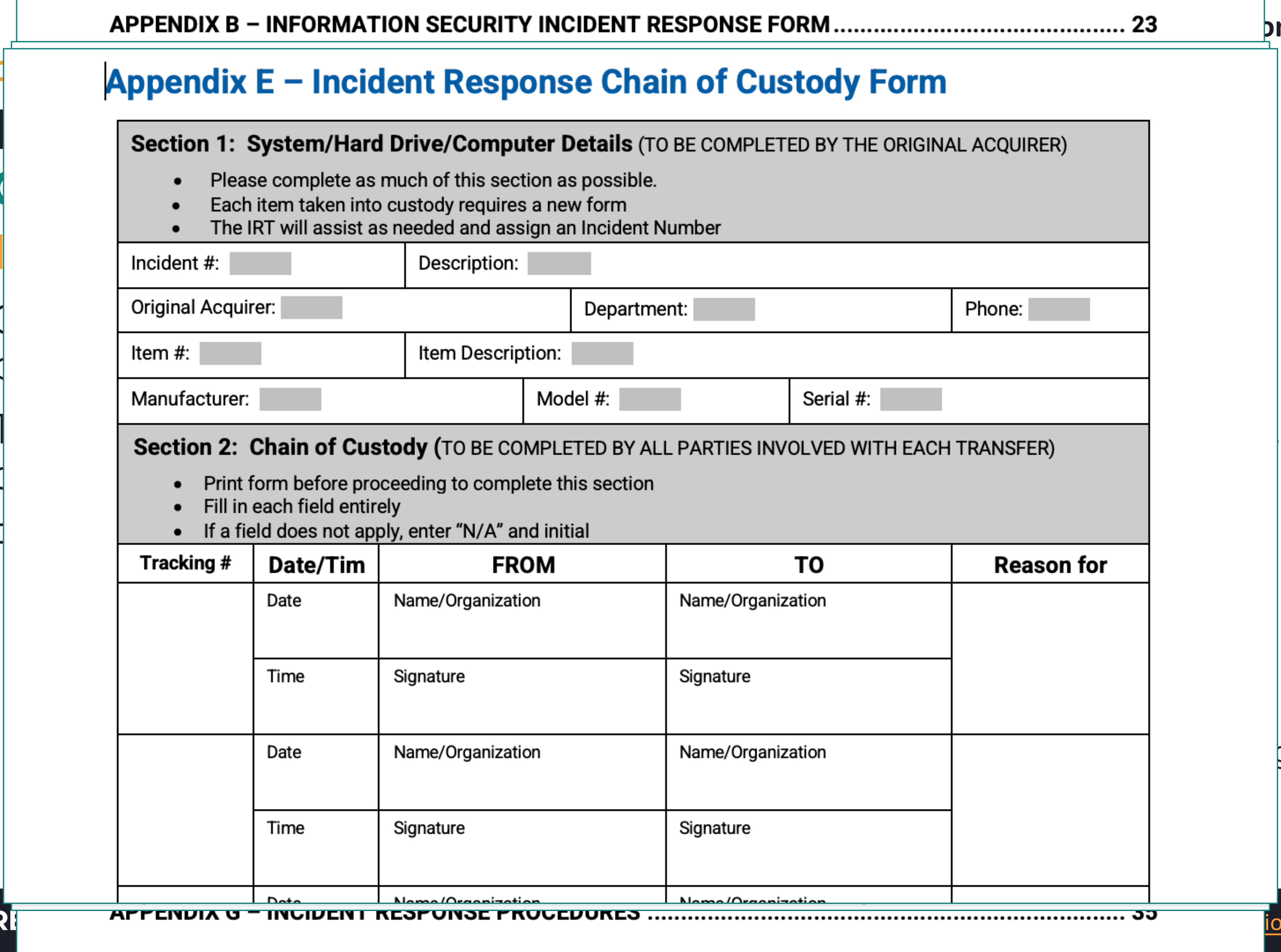
- Please complete as much of this section as possible.
- Each item taken into custody requires a new form
- The IRT will assist as needed and assign an Incident Number

Incident #:	Description:	
Original Acquirer:	Department:	Phone:
Item #:	Item Description:	
Manufacturer:	Model #:	Serial #:

Section 2: Chain of Custody (TO BE COMPLETED BY ALL PARTIES INVOLVED WITH EACH TRANSFER)

- Print form before proceeding to complete this section
- Fill in each field entirely
- If a field does not apply, enter "N/A" and initial

Tracking #	Date/Tim	FROM	TO	Reason for
	Date	Name/Organization	Name/Organization	
	Time	Signature	Signature	
	Date	Name/Organization	Name/Organization	
	Time	Signature	Signature	
	Date	Name/Organization	Name/Organization	



Appendix E – Incident Response Chain of Custody Form

Section 1: System/Hard Drive/Computer Details (TO BE COMPLETED BY THE ORIGINAL ACQUIRER)

- Please complete as much of this section as possible.
- Each item taken into custody requires a new form
- The IRT will assist as needed and assign an Incident Number

Incident #:

Description:

Original Acquirer:

Department:

Phone:

Item #:

Item Description:

Manufacturer:

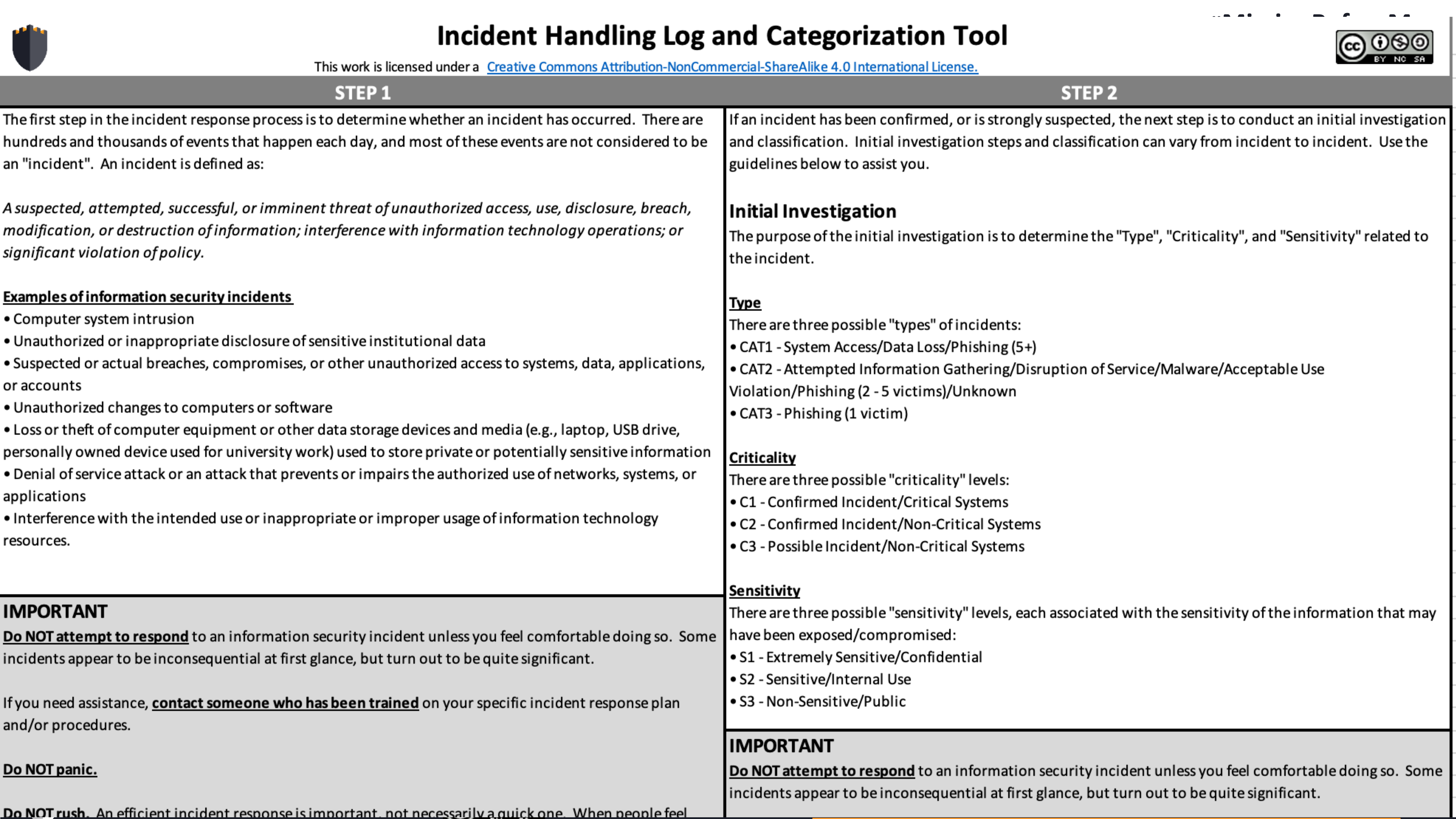
Model #:

Serial #:

Section 2: Chain of Custody (TO BE COMPLETED BY ALL PARTIES INVOLVED WITH EACH TRANSFER)

- Print form before proceeding to complete this section
- Fill in each field entirely
- If a field does not apply, enter "N/A" and initial

Tracking #	Date/Tim	FROM	TO	Reason for
	Date	Name/Organization	Name/Organization	
	Time	Signature	Signature	
	Date	Name/Organization	Name/Organization	
	Time	Signature	Signature	
	Date	Name/Organization	Name/Organization	



Incident Handling Log and Categorization Tool

STEP 1

The first step in the incident response process is to determine whether an incident has occurred. There are hundreds and thousands of events that happen each day, and most of these events are not considered to be an "incident". An incident is defined as:

A suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of policy.

Examples of information security incidents

- Computer system intrusion
- Unauthorized or inappropriate disclosure of sensitive institutional data
- Suspected or actual breaches, compromises, or other unauthorized access to systems, data, applications, or accounts
- Unauthorized changes to computers or software
- Loss or theft of computer equipment or other data storage devices and media (e.g., laptop, USB drive, personally owned device used for university work) used to store private or potentially sensitive information
- Denial of service attack or an attack that prevents or impairs the authorized use of networks, systems, or applications
- Interference with the intended use or inappropriate or improper usage of information technology resources.

IMPORTANT

Do NOT attempt to respond to an information security incident unless you feel comfortable doing so. Some incidents appear to be inconsequential at first glance, but turn out to be quite significant.

If you need assistance, **contact someone who has been trained** on your specific incident response plan and/or procedures.

Do NOT panic.

Do NOT rush. An efficient incident response is important, not necessarily a quick one. When people feel

STEP 2

If an incident has been confirmed, or is strongly suspected, the next step is to conduct an initial investigation and classification. Initial investigation steps and classification can vary from incident to incident. Use the guidelines below to assist you.

Initial Investigation

The purpose of the initial investigation is to determine the "Type", "Criticality", and "Sensitivity" related to the incident.

Type

There are three possible "types" of incidents:

- CAT1 - System Access/Data Loss/Phishing (5+)
- CAT2 - Attempted Information Gathering/Disruption of Service/Malware/Acceptable Use Violation/Phishing (2 - 5 victims)/Unknown
- CAT3 - Phishing (1 victim)

Criticality

There are three possible "criticality" levels:

- C1 - Confirmed Incident/Critical Systems
- C2 - Confirmed Incident/Non-Critical Systems
- C3 - Possible Incident/Non-Critical Systems

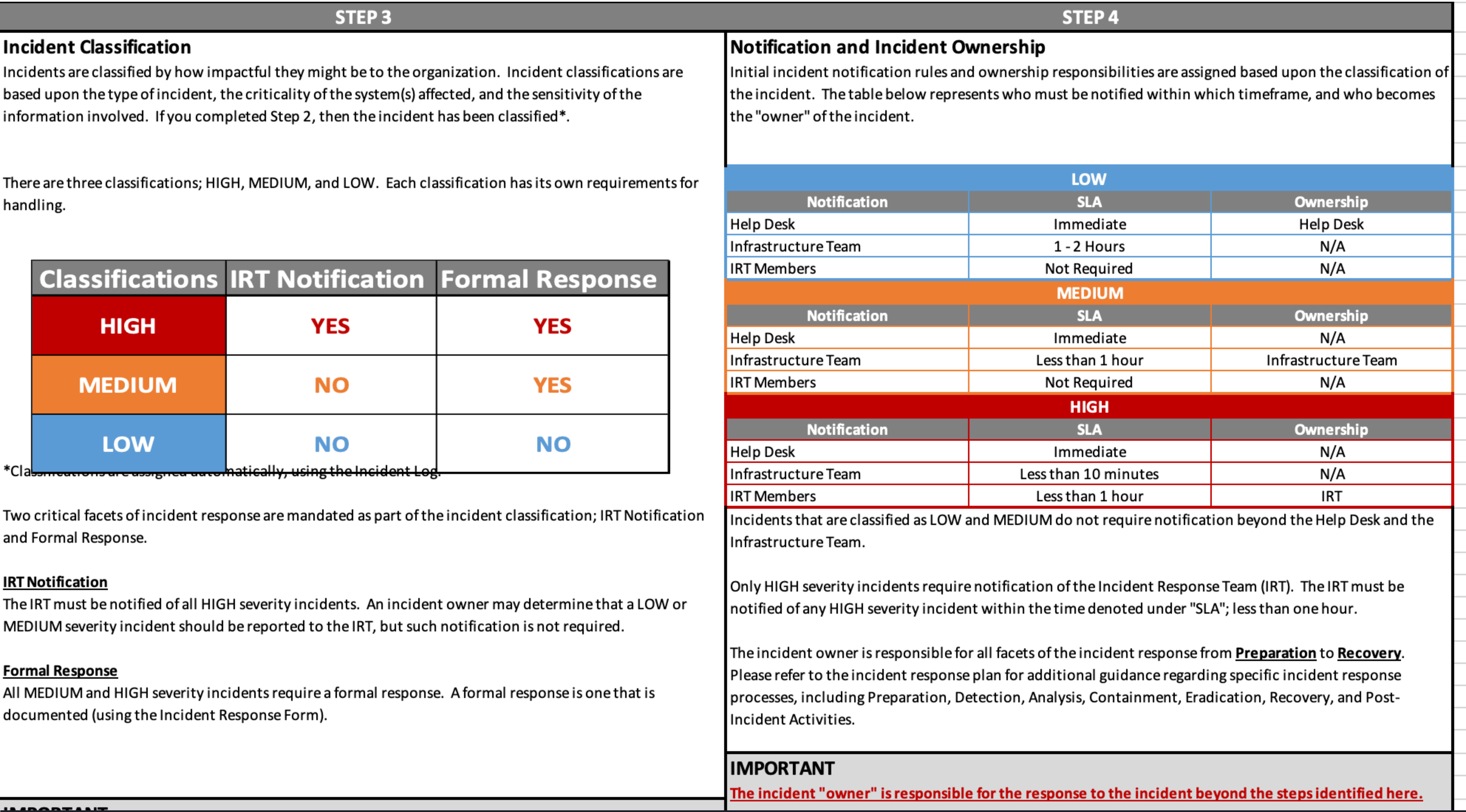
Sensitivity

There are three possible "sensitivity" levels, each associated with the sensitivity of the information that may have been exposed/compromised:

- S1 - Extremely Sensitive/Confidential
- S2 - Sensitive/Internal Use
- S3 - Non-Sensitive/Public

IMPORTANT

Do NOT attempt to respond to an information security incident unless you feel comfortable doing so. Some incidents appear to be inconsequential at first glance, but turn out to be quite significant.



STEP 3

Incident Classification

Incidents are classified by how impactful they might be to the organization. Incident classifications are based upon the type of incident, the criticality of the system(s) affected, and the sensitivity of the information involved. If you completed Step 2, then the incident has been classified*.

There are three classifications; HIGH, MEDIUM, and LOW. Each classification has its own requirements for handling.

Classifications	IRT Notification	Formal Response
HIGH	YES	YES
MEDIUM	NO	YES
LOW	NO	NO

*Classifications are assigned automatically, using the Incident Log.

Two critical facets of incident response are mandated as part of the incident classification; IRT Notification and Formal Response.

IRT Notification

The IRT must be notified of all HIGH severity incidents. An incident owner may determine that a LOW or MEDIUM severity incident should be reported to the IRT, but such notification is not required.

Formal Response

All MEDIUM and HIGH severity incidents require a formal response. A formal response is one that is documented (using the Incident Response Form).

IMPORTANT

STEP 4

Notification and Incident Ownership

Initial incident notification rules and ownership responsibilities are assigned based upon the classification of the incident. The table below represents who must be notified within which timeframe, and who becomes the "owner" of the incident.

LOW		
Notification	**SLA**	**Ownership**
Help Desk	Immediate	Help Desk
Infrastructure Team	1 - 2 Hours	N/A
IRT Members	Not Required	N/A
MEDIUM		
Notification	**SLA**	**Ownership**
Help Desk	Immediate	N/A
Infrastructure Team	Less than 1 hour	Infrastructure Team
IRT Members	Not Required	N/A
HIGH		
Notification	**SLA**	**Ownership**
Help Desk	Immediate	N/A
Infrastructure Team	Less than 10 minutes	N/A
IRT Members	Less than 1 hour	IRT

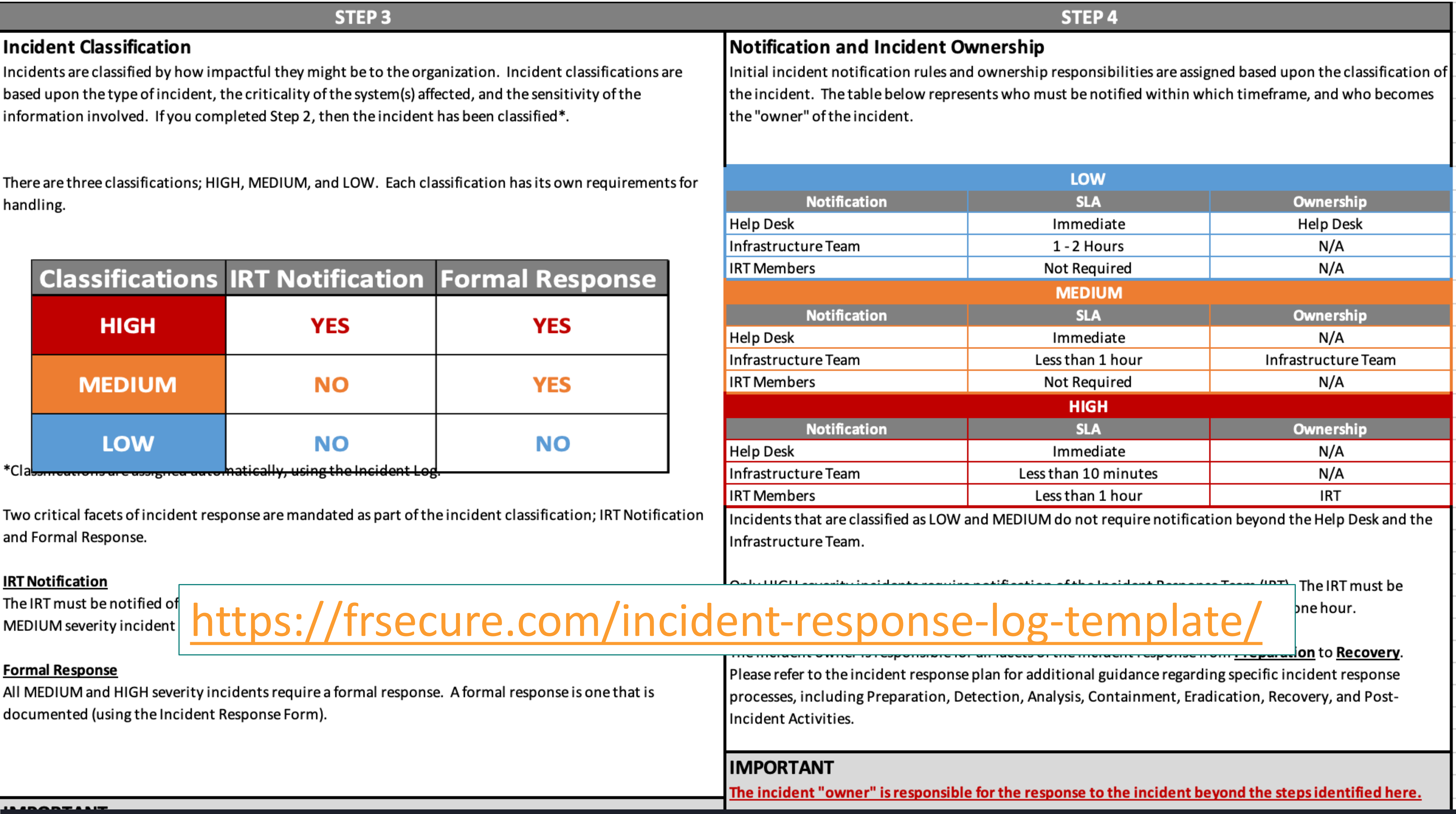
Incidents that are classified as LOW and MEDIUM do not require notification beyond the Help Desk and the Infrastructure Team.

Only HIGH severity incidents require notification of the Incident Response Team (IRT). The IRT must be notified of any HIGH severity incident within the time denoted under "SLA"; less than one hour.

The incident owner is responsible for all facets of the incident response from **Preparation** to **Recovery**. Please refer to the incident response plan for additional guidance regarding specific incident response processes, including Preparation, Detection, Analysis, Containment, Eradication, Recovery, and Post-Incident Activities.

IMPORTANT

The incident "owner" is responsible for the response to the incident beyond the steps identified here.



STEP 3

Incident Classification

Incidents are classified by how impactful they might be to the organization. Incident classifications are based upon the type of incident, the criticality of the system(s) affected, and the sensitivity of the information involved. If you completed Step 2, then the incident has been classified*.

There are three classifications; HIGH, MEDIUM, and LOW. Each classification has its own requirements for handling.

Classifications	IRT Notification	Formal Response
HIGH	YES	YES
MEDIUM	NO	YES
LOW	NO	NO

*Classifications are assigned automatically, using the Incident Log.

Two critical facets of incident response are mandated as part of the incident classification; IRT Notification and Formal Response.

IRT Notification

The IRT must be notified of

MEDIUM severity incident

Formal Response

All MEDIUM and HIGH severity incidents require a formal response. A formal response is one that is documented (using the Incident Response Form).

IMPORTANT

STEP 4

Notification and Incident Ownership

Initial incident notification rules and ownership responsibilities are assigned based upon the classification of the incident. The table below represents who must be notified within which timeframe, and who becomes the "owner" of the incident.

LOW		
Notification	**SLA**	**Ownership**
Help Desk	Immediate	Help Desk
Infrastructure Team	1 - 2 Hours	N/A
IRT Members	Not Required	N/A
MEDIUM		
Notification	**SLA**	**Ownership**
Help Desk	Immediate	N/A
Infrastructure Team	Less than 1 hour	Infrastructure Team
IRT Members	Not Required	N/A
HIGH		
Notification	**SLA**	**Ownership**
Help Desk	Immediate	N/A
Infrastructure Team	Less than 10 minutes	N/A
IRT Members	Less than 1 hour	IRT

Incidents that are classified as LOW and MEDIUM do not require notification beyond the Help Desk and the Infrastructure Team.

Only HIGH severity incidents require notification of the Incident Response Team (IRT). The IRT must be one hour.

The incident owner is responsible for all facets of the incident response from **Preparation** to **Recovery**. Please refer to the incident response plan for additional guidance regarding specific incident response processes, including Preparation, Detection, Analysis, Containment, Eradication, Recovery, and Post-Incident Activities.

IMPORTANT

The incident "owner" is responsible for the response to the incident beyond the steps identified here.

https://frsecure.com/incident-response-log-template/

STEP 3

STEP 4

Incident Classification

Incidents are classified by ho

based upon the type of incid

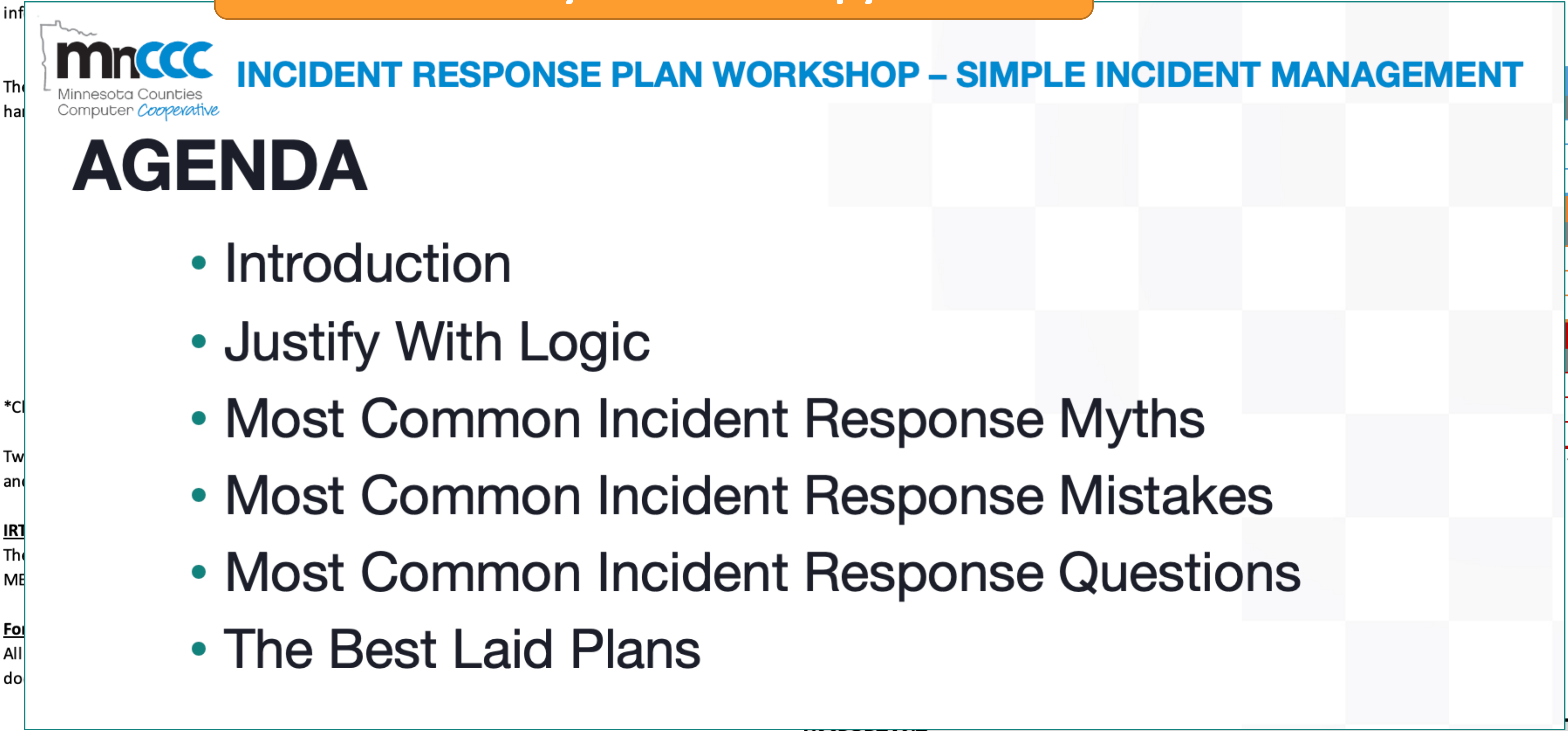
inf

Notification and Incident Ownership

wnership responsibilities are assigned based upon the classification of

ts who must be notified within which timeframe, and who becomes

Let me know if you want a copy of this...



INCIDENT RESPONSE PLAN WORKSHOP – SIMPLE INCIDENT MANAGEMENT

mnCCC Minnesota Counties Computer Cooperative

AGENDA

- Introduction
- Justify With Logic
- Most Common Incident Response Myths
- Most Common Incident Response Mistakes
- Most Common Incident Response Questions
- The Best Laid Plans

Th

ha

*Cl

Tw

an

IRT

Th

ME

Fo

All

do

the

IMPORTANT

The incident "owner" is responsible for the response to the incident beyond the steps identified here.

IMPORTANT

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT INCIDENT MANAGEMENT

Incident Response Testing and Exercise

Testing is mandatory.

Excellent training opportunities.

Improves response.

Can be used to integrate with other plans.

CISSP® MENTOR PROGRAM – SESSION TEN

DOMAIN 7 – SECURITY OPERATIONS

CONDUCT INCIDENT MANAGEMENT

Incident Response - Reporting

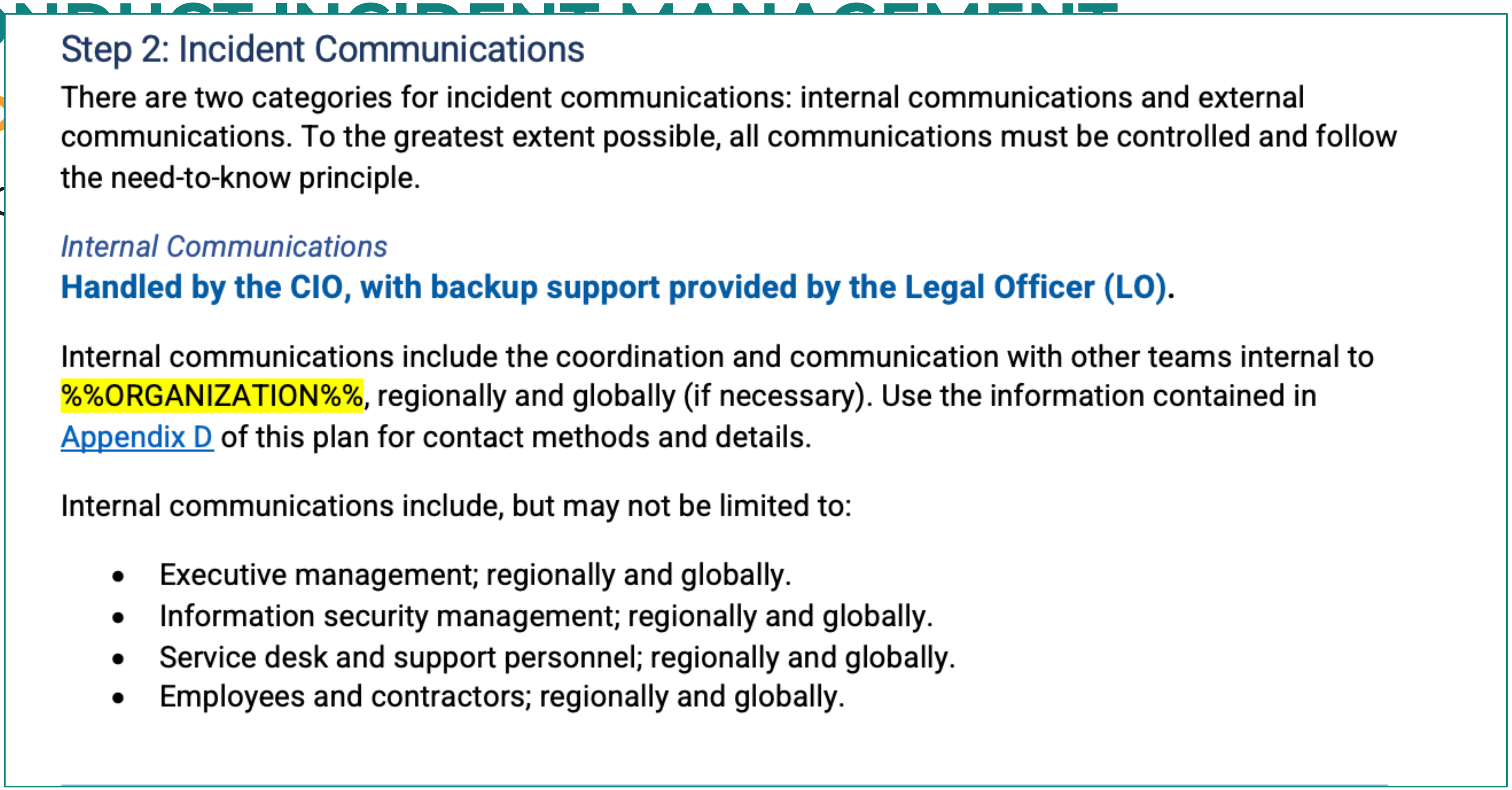
Two messages, one internal and the other external.

DOMAIN 7 – SECURITY OPERATIONS

CO

Inc

Tw



Step 2: Incident Communications

There are two categories for incident communications: internal communications and external communications. To the greatest extent possible, all communications must be controlled and follow the need-to-know principle.

Internal Communications

Handled by the CIO, with backup support provided by the Legal Officer (LO).

Internal communications include the coordination and communication with other teams internal to %%ORGANIZATION%%, regionally and globally (if necessary). Use the information contained in Appendix D of this plan for contact methods and details.

Internal communications include, but may not be limited to:

- Executive management; regionally and globally.
- Information security management; regionally and globally.
- Service desk and support personnel; regionally and globally.
- Employees and contractors; regionally and globally.

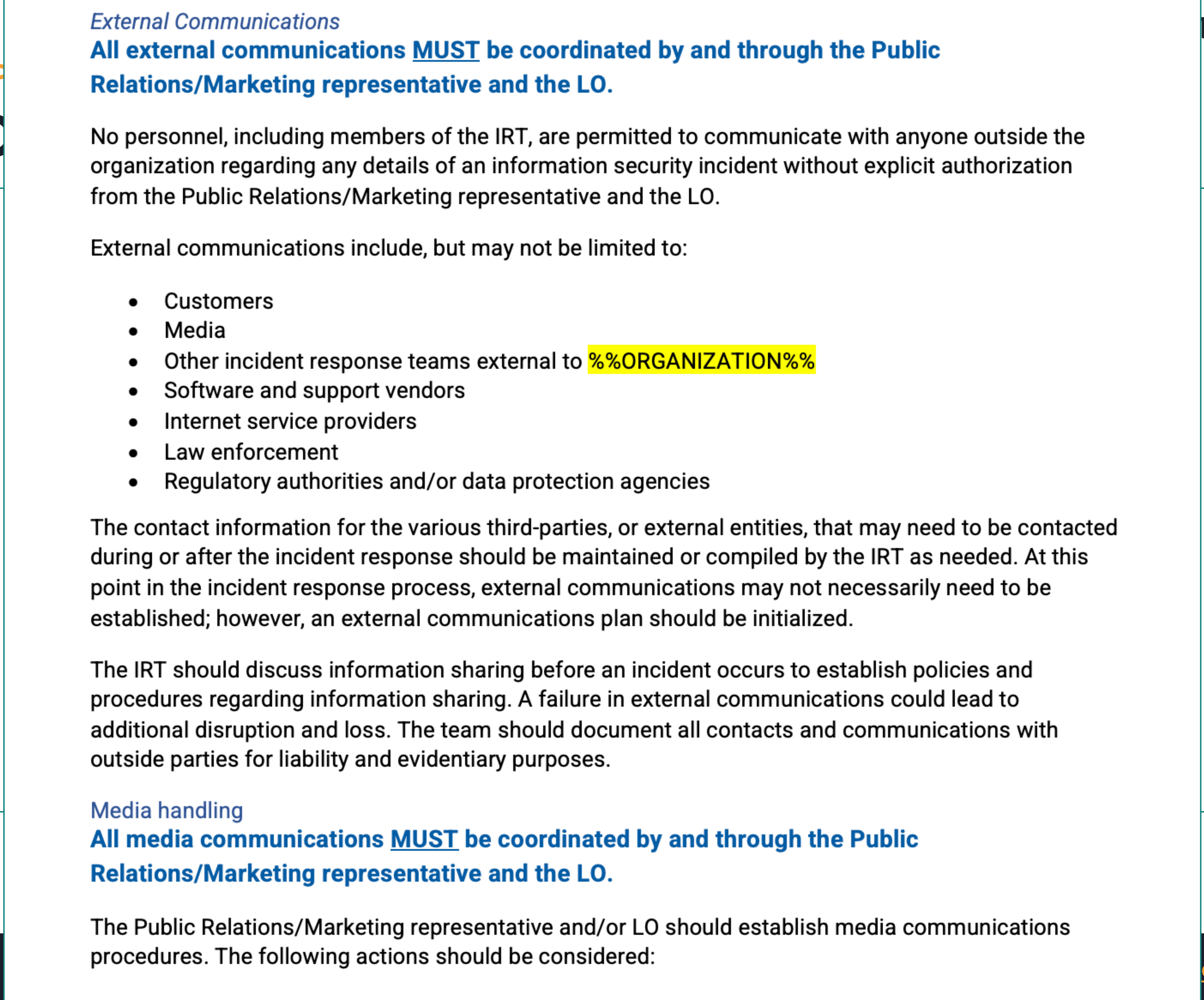
CISSP

DO

CO

Inc

Two



External Communications

All external communications <u>MUST</u> be coordinated by and through the Public Relations/Marketing representative and the LO.

No personnel, including members of the IRT, are permitted to communicate with anyone outside the organization regarding any details of an information security incident without explicit authorization from the Public Relations/Marketing representative and the LO.

External communications include, but may not be limited to:

- Customers
- Media
- Other incident response teams external to %%ORGANIZATION%%
- Software and support vendors
- Internet service providers
- Law enforcement
- Regulatory authorities and/or data protection agencies

The contact information for the various third-parties, or external entities, that may need to be contacted during or after the incident response should be maintained or compiled by the IRT as needed. At this point in the incident response process, external communications may not necessarily need to be established; however, an external communications plan should be initialized.

The IRT should discuss information sharing before an incident occurs to establish policies and procedures regarding information sharing. A failure in external communications could lead to additional disruption and loss. The team should document all contacts and communications with outside parties for liability and evidentiary purposes.

Media handling

All media communications <u>MUST</u> be coordinated by and through the Public Relations/Marketing representative and the LO.

The Public Relations/Marketing representative and/or LO should establish media communications procedures. The following actions should be considered:

CISSP® MENTOR PROGRAM – SESSION TEN

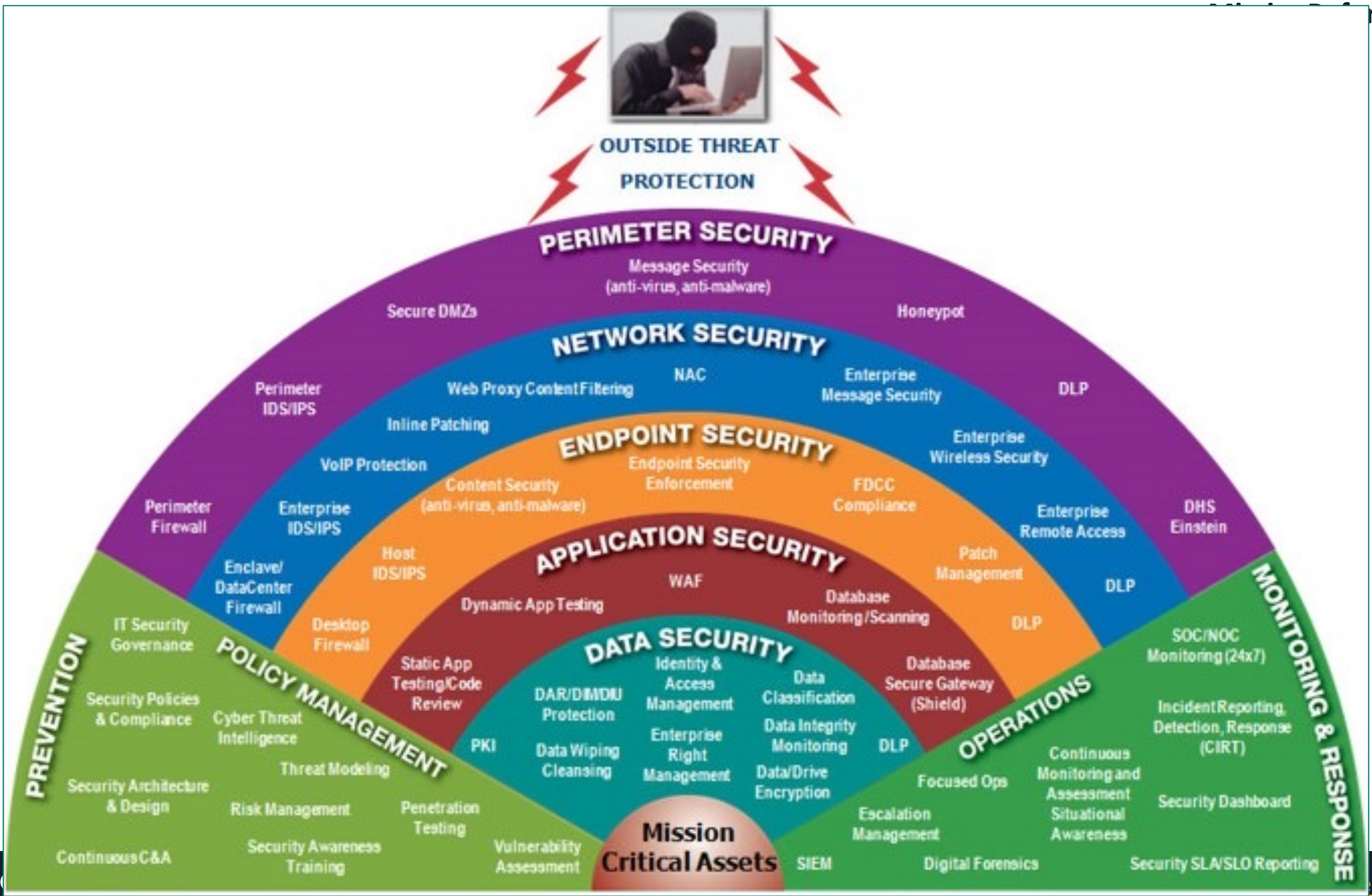
DOMAIN 7 – SECURITY OPERATIONS

OPERATE AND MAINTAIN DETECTIVE AND PREVENTATIVE MEASURES

DOMAIN 7 – SECURITY OPERATIONS

OPERATE AND MAINTAIN DETECTIVE AND PREVENTATIVE MEASURES

Defense-in-depth where controls are layered to serve both preventative and detective functions.


OUTSIDE THREAT
PROTECTION
PERIMETER SECURITY
Message Security (anti-virus, anti-malware)
Secure DMZs
Honeypot
Perimeter IDS/IPS
DLP
Perimeter Firewall
DHS Einstein
NETWORK SECURITY
Web Proxy Content Filtering
NAC
Enterprise Message Security
Inline Patching
VoIP Protection
Enterprise Wireless Security
Enterprise IDS/IPS
Enterprise Remote Access
Enclave/ DataCenter Firewall
DLP
ENDPOINT SECURITY
Endpoint Security Enforcement
Content Security (anti-virus, anti-malware)
FDCC Compliance
Host IDS/IPS
Patch Management
Desktop Firewall
DLP
APPLICATION SECURITY
WAF
Dynamic App Testing
Database Monitoring/Scanning
Static App Testing/Code Review
Database Secure Gateway (Shield)
DATA SECURITY
Identity & Access Management
DAR/DIM/DIU Protection
Data Classification
Enterprise Right Management
Data Integrity Monitoring
PKI
Data Wiping Cleansing
Data/Drive Encryption
DLP
Mission Critical Assets
PREVENTION
IT Security Governance
Security Policies & Compliance
Security Architecture & Design
Continuous C&A
POLICY MANAGEMENT
Cyber Threat Intelligence
Threat Modeling
Risk Management
Penetration Testing
Security Awareness Training
Vulnerability Assessment
MONITORING & RESPONSE
SOC/NOC Monitoring (24x7)
Incident Reporting, Detection, Response (CIRT)
Security Dashboard
Security SLA/SLO Reporting
OPERATIONS
Continuous Monitoring and Assessment
Situational Awareness
Focused Ops
Escalation Management
Digital Forensics
SIEM

https://nsacyber.github.io/publications.html

National Security Agency/Central Security Service

INFORMATION
ASSURANCE
DIRECTORATE

NSA Methodology for Adversary Obstruction

DOMAIN 7 – SECURITY OPERATIONS

OPERATE AND MAINTAIN DETECTIVE AND PREVENTATIVE MEASURES

Firewalls (review)

- **Static packet inspection** (stateless)
- **Stateful packet inspection**
- **Web application firewall (WAF) and API gateway** - Specialized network access control devices designed to handle specific types of traffic, unlike a generic firewall that handles all network traffic. WAFs and API gateways analyze traffic destined specifically for a web application or an application's API.
- **Host-based firewalls** - These are installed on a specific endpoint and use a ruleset specific to that endpoint.

DOMAIN 7 – SECURITY OPERATIONS

OPERATE AND MAINTAIN DETECTIVE AND PREVENTATIVE MEASURES

Firewalls (review)

- **Next-generation firewalls (NGFW)** - These are more of a marketing term than a unique type of firewall. Combines network security services into a single device/system. Lower overhead and cost (maybe), but higher complexity in a single device (point of failure).
- **Security groups**: These exist in software defined networks (SDNs) and cloud environments and serve many of the same functions as a firewall.

Firewalls, security groups, and microsegmentation are useful access control devices in a zero-trust network architecture, where no part of the network is implicitly trusted.

DOMAIN 7 – SECURITY OPERATIONS

OPERATE AND MAINTAIN DETECTIVE AND PREVENTATIVE MEASURES

Intrusion Detection Systems and Intrusion Prevention Systems

Nothing new to cover here.

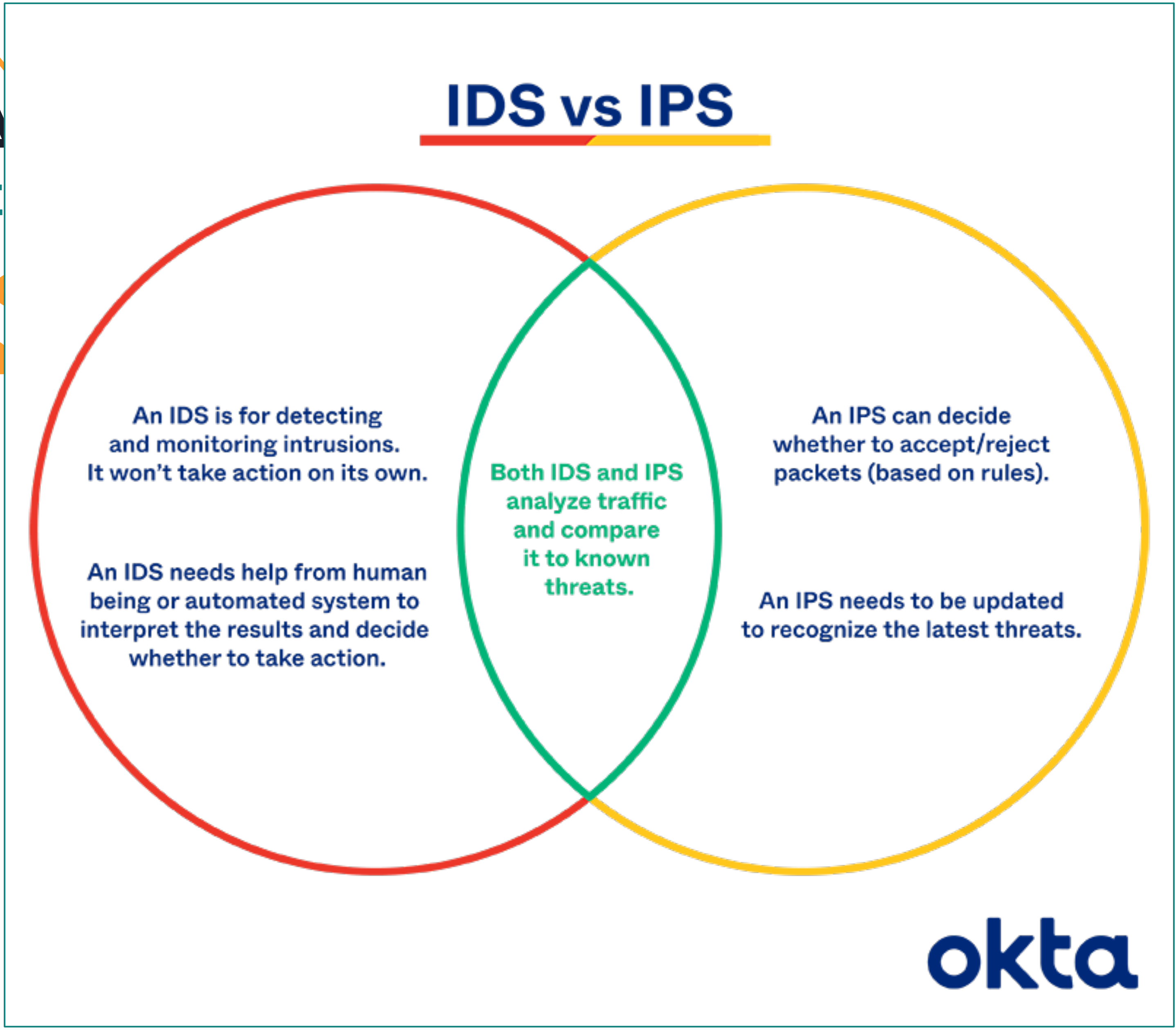
CISSP® MEN

DOMA

OPERATE EASURES

Intrusi
Preven

Nothing



IDS vs IPS

An IDS is for detecting and monitoring intrusions. It won't take action on its own.

An IDS needs help from human being or automated system to interpret the results and decide whether to take action.

Both IDS and IPS analyze traffic and compare it to known threats.

An IPS can decide whether to accept/reject packets (based on rules).

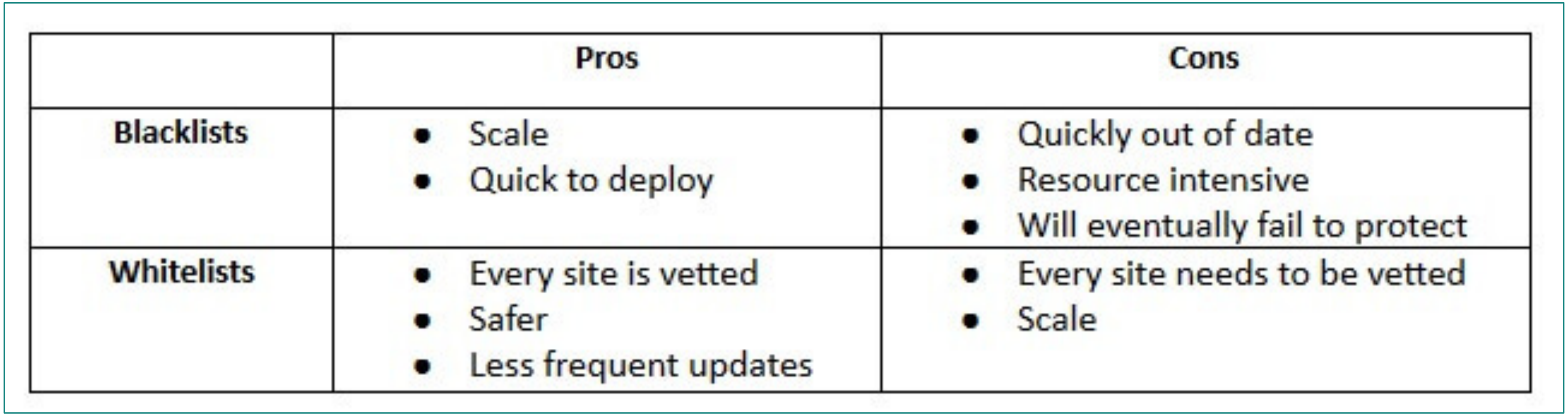
An IPS needs to be updated to recognize the latest threats.

DOMAIN 7 – SECURITY OPERATIONS

OPERATE AND MAINTAIN DETECTIVE AND PREVENTATIVE MEASURES

Whitelisting/Blacklisting

Mostly changed to allowlisting and blocklisting.



	Pros	Cons
Blacklists	• Scale • Quick to deploy	• Quickly out of date • Resource intensive • Will eventually fail to protect
Whitelists	• Every site is vetted • Safer • Less frequent updates	• Every site needs to be vetted • Scale

DOMAIN 7 – SECURITY OPERATIONS

OPERATE AND MAINTAIN DETECTIVE AND PREVENTATIVE MEASURES

Third-Party-Provided Security Services

- Pros and Cons

Common services:

- **Security Operations Center (SOC)**: Full or partial SOC outsourcing can be useful to deal with the cost and complexity of building and running a 24x7 SOC operation.
- **Digital Forensics and Incident Response (DFIR):** look for orgs without bias.
- **Threat intelligence:** can provide useful information about threats that could target the organization and are often industry- or technology-specific.

DOMAIN 7 – SECURITY OPERATIONS

OPERATE AND MAINTAIN DETECTIVE AND PREVENTATIVE MEASURES

Sandboxing

- Run code, observe and analyze and code in a safe, isolated environment on a network that mimics end-user operating environments.
- Designed to prevent threats from getting on the network and is frequently used to inspect untested or untrusted code.

Honeypots/Honeynets

- Network-attached system as a decoy to lure cyber attackers.
- Used to detect, deflect and study hacking attempts to gain unauthorized access to information systems.
- A honeynet is a collection of honeypots.

DOMAIN 7 – SECURITY OPERATIONS

OPERATE AND MAINTAIN DETECTIVE AND PREVENTATIVE MEASURES

Be careful with honeypots, entrapment versus enticement.

- Designed to prevent threats from getting on the network and is frequently used to inspect untested or untrusted code.

Honeypots/Honeynets

- Network-attached system as a decoy to lure cyber attackers.
- Used to detect, deflect and study hacking attempts to gain unauthorized access to information systems.
- A honeynet is a collection of honeypots.

CISSP® MENTOR PROGRAM – SESSION TEN

DOMAIN 7 – SECURITY OPERATIONS

IMPLEMENT AND SUPPORT PATCH AND VULNERABILITY MANAGEMENT

DOMAIN 7 – SECURITY OPERATIONS

IMPLEMENT AND SUPPORT PATCH AND VULNERABILITY MANAGEMENT

Five crazy facts on exactly how much time is spent on debugging and code fixing in the software industry:

1. On average, a developer creates 70 bugs per 1000 lines of code (!)
2. 15 bugs per 1,000 lines of code find their way to the customers
3. Fixing a bug takes 30 times longer than writing a line of code
4. 75% of a developer's time is spent on debugging (1500 hours a year!)
5. In the US alone, $113B is spent annually on identifying & fixing product defects

DOMAIN 7 – SECURITY OPERATIONS

IMPLEMENT AND SUPPORT PATCH AND VULNERABILITY MANAGEMENT

Five crazy facts on exactly how much time is spent on debugging and code fixing in the software industry:

1. On average, a developer creates 70 bugs per 1000 lines of code (!)
2. 15 bugs per 1,000 lines of code find their way to the customers
3. Fixing a bug takes 30 times longer than writing a line of code
4. 75% of a developer's time is spent on debugging (1500 hours a year!)
5. In the US alone, $113B is spent annually on identifying & fixing product defects

Windows 10, 50MM LOC, 75,000 Bugs?!

The average car, according to KPMG, has over 150 Million lines of code in it.

DOMAIN 7 – SECURITY OPERATIONS

IMPLEMENT AND SUPPORT PATCH AND VULNERABILITY MANAGEMENT

Patch Management

A generic security patch process incorporating all stakeholders must include the following:

Vulnerability detection – Scanning, researcher, user reporting a bug, etc.

Patch publication - By the vendor or development team, once the vulnerability is verified and relevant code is written to address it.

Evaluation - Patch applicability by each organization's administrative personnel to determine if the patch is needed in each environment.

Testing - Ensure the patch won't introduce problems.

Apply and Track - Ensure the patch doesn't have a negative impact on functionality.

Rollback - If issues are encountered.

Documentation - Of the system including the patch, which becomes the

CISSP® MENTOR PROGRAM – SESSION TEN

DOMAIN 7 – SECURITY OPERATIONS

UNDERSTAND AND PARTICIPATE IN CHANGE MANAGEMENT PROCESSES

This is where we'll stop for the night…

CISSP® MEN

DOMA

UNDERST PROCESSES

This is w

SESSION TEN – POR FIN!

Homework:

- Catchup in you reading. You should be through (or at least beginning) Domain 7 soon.
- Take practice tests.
- Review at least two of the references we provided in this class (download for later use).
- Post at least one question/answer in the Slack Channel.

See you Monday!

FRSecure CISSP Mentor Program

2022

Class #10 – Domain 7

Evan Francen

Evan Francen – FRSecure and SecurityStudio Co-Founder & CEO