# Designing and Using Security Exercises to Test and Improve Security Programs

Marc N. Violante

Wisconsin Procurement Institute

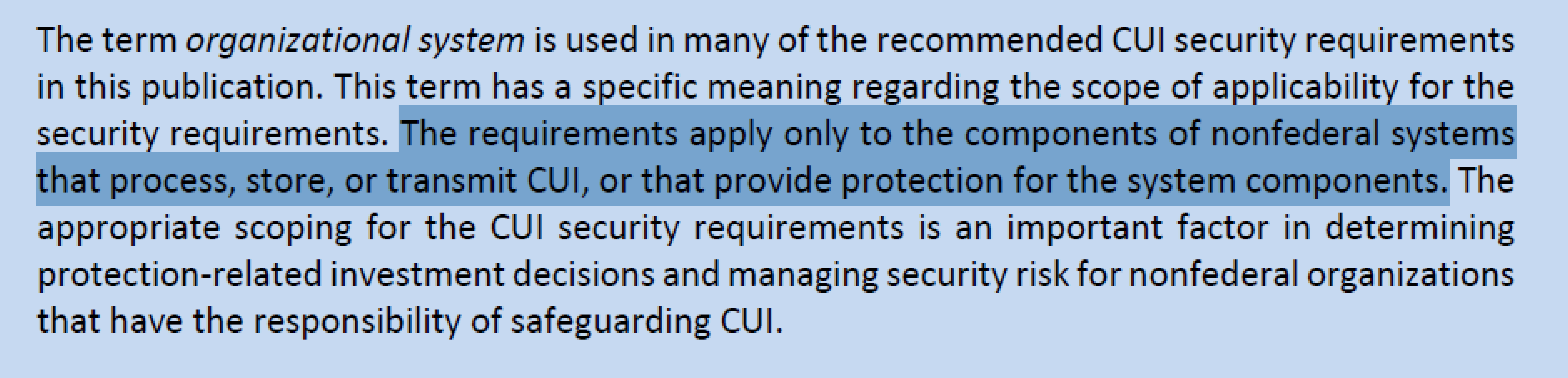
December 2, 2022

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

# Webinar Description

- Cybersecurity plans are developed with the best of intentions, the utmost care, and are stored "on the shelf" ready to go. Are they functional and have they been developed in a manner to deal with typical cyber incidents and attacks? Planning and hoping for the best is one strategy – but not a very effective one. There are a variety of other strategies that will support a stronger program such as penetration testing, external phishing campaigns (ransomware and other), and even physical disruption to the network to trigger the incident response plan. These options, though, require contracting with specialized firms to perform a limited scope of work. Due to cost and scheduling limitations, they are often not practical.
- Alternatively, a company can utilize internally developed and managed exercises to test their cyber incident response capabilities for any number of incidents. Exercises provide two important pieces of feedback. First, an exercise will provide valuable information on how well the company's Incident Response plan functions and secondly, the exercise will test the staff's knowledge of the plan and their duties within the plan.
- This webinar will discuss the basic design of an exercise, available resources and related considerations.

# The meaning of organizational system



The term *organizational system* is used in many of the recommended CUI security requirements in this publication. This term has a specific meaning regarding the scope of applicability for the security requirements. The requirements apply only to the components of nonfederal systems that process, store, or transmit CUI, or that provide protection for the system components. The appropriate scoping for the CUI security requirements is an important factor in determining protection-related investment decisions and managing security risk for nonfederal organizations that have the responsibility of safeguarding CUI.

SP 800-171, REVISION 2 PROTECTING CONTROLLED UNCLASSIFIED INFORMATION, page 10

# What data is maintained?

What data is used, managed, stored?

What data has reporting requirements?

Identify the reporting requirements?

What data is required for the reports?

Are there specified report formats?

Are there other reporting requirements – time,

# Meet Murphy

*The day was perfect until …*

*What do we do now?*

# Develop an Exercise Program

1. Conduct assessment of needs and current capabilities to include
   - Policies, Procedures and Practices
2. Review the Risk Assessment
3. Review Performance Objectives
4. Conduct a Walkthrough / Orientation
5. Review Roles and Responsibilities
6. Identify probable scenarios for emergencies and business disruption

https://www.ready.gov/exercises

# Exercises

- Exercises should be designed to engage team members and get them working together to manage the response to a hypothetical incident.
- Exercises
  - enhance knowledge of plans,
  - allow members to improve their own performance
  - and identify opportunities to improve capabilities to respond to real events.

https://www.ready.gov/exercises

# More is not always better

- A common misconception is that scenarios must be very detailed to be effective.
- Actually, it is often more effective to develop a short, concise scenario.
- During tabletop exercises with long, detailed scenarios, participants often spend more time dissecting the scenario and discussing its content than they spend on meeting the objectives of the exercise.
- If a detailed scenario is desired, a trusted agent with detailed knowledge of the plan and all the procedures documented within the plan should aid in the development of the scenario to ensure accuracy.
- In addition, the facilitator should have the ability to redirect the participants' focus from the scenario to the objectives, should they begin focusing too much on the content of the scenario.

GUIDE TO TEST,TRAINING, AND EXERCISE PROGRAMS FOR ITPLANS AND CAPABILITIES, NIST SP 800-84, page 4-4

# Types of Exercises

Walkthroughs, workshops or orientation seminars

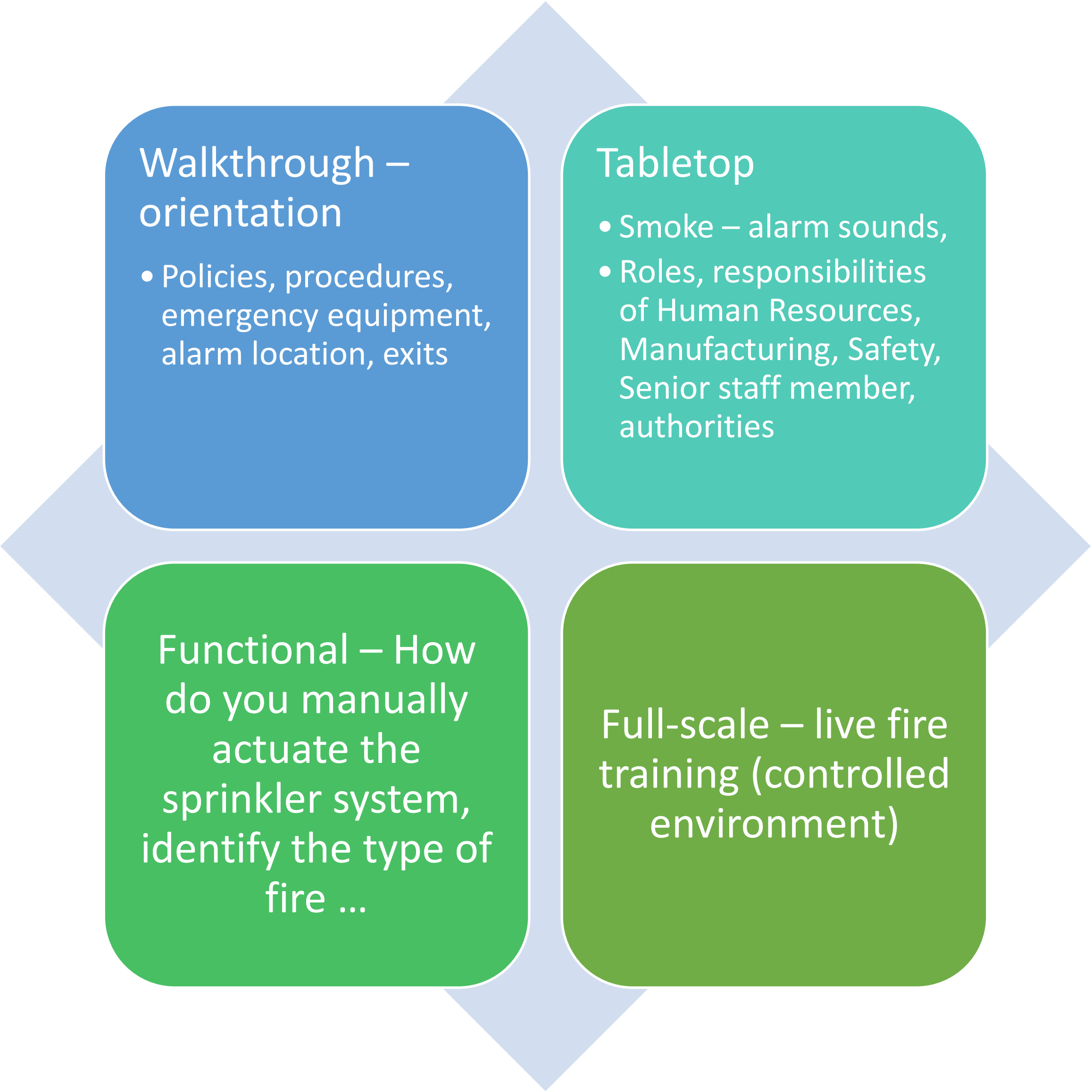
Tabletop exercises

Functional exercises

Full-scale exercises

https://www.ready.gov/exercises

# Fire Scenario



## Walkthrough – orientation

- Policies, procedures, emergency equipment, alarm location, exits

## Tabletop

- Smoke – alarm sounds,
- Roles, responsibilities of Human Resources, Manufacturing, Safety, Senior staff member, authorities

Functional – How do you manually actuate the sprinkler system, identify the type of fire …

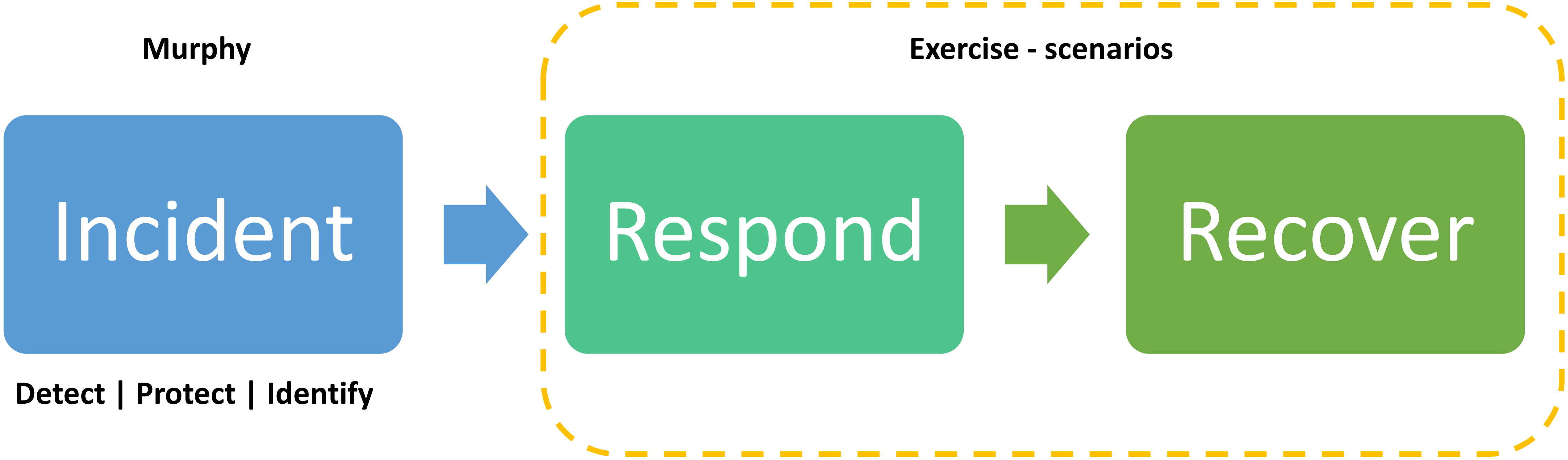
Full-scale – live fire training (controlled environment)

# Exercise elements

- Review the plan
- Define the goal
- Form exercise development team
- Develop objective
- Develop scenario
- Identify Players
- Identify Participants
- Decide on format
- Develop scripts and injects

Ready.gov/exercises

# Exercise Domain



Murphy

Exercise - scenarios

Incident

Respond

Recover

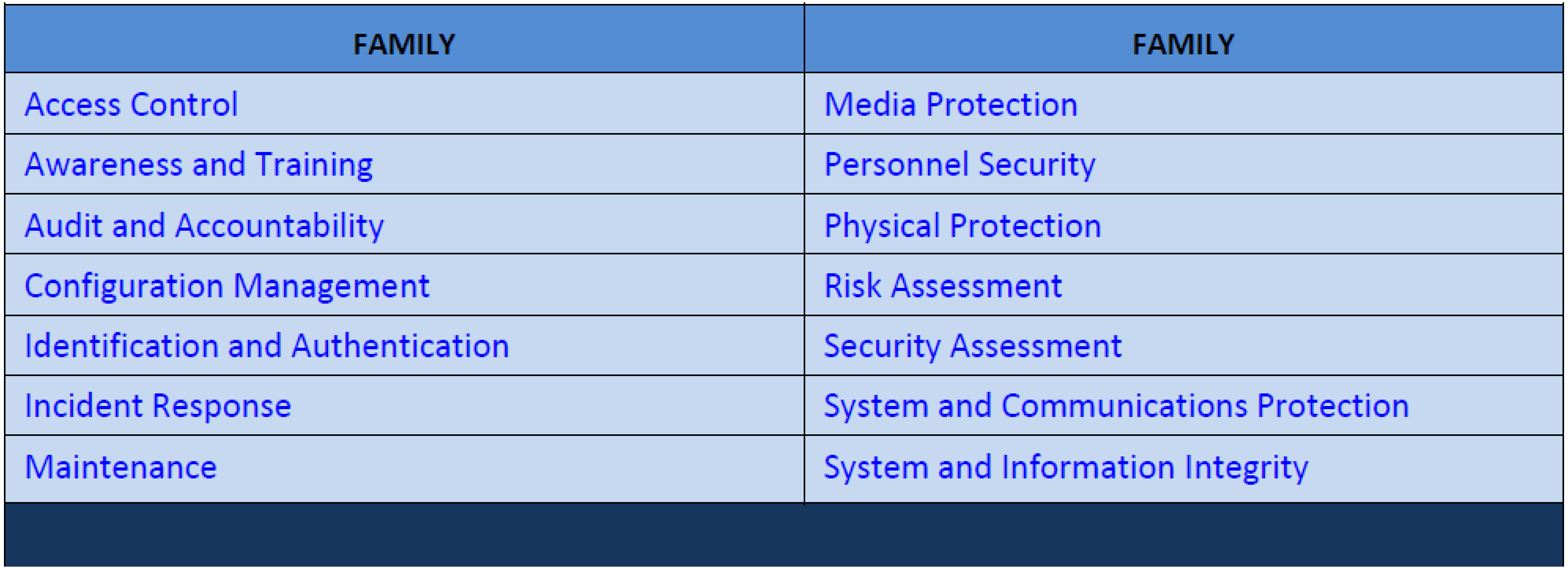
Detect | Protect | Identify

NIST Cybersecurity Framework, Apr 16, 2018, V1.1

# Develop a Risk Matrix

| Business Risk | Likelihood | Likely Impact | Plan |
|---|---|---|---|
| Cyber Incident | High | High | Yes |
| Fire | Low | Medium | No |
| Insider Threat | Low | High | No |
| Key Person | Medium | Medium | No |
| Major Power Outage | Low | High | No |
| Network Outage | Medium | High | No |
| | | | |

# Scenario topic areas



| FAMILY | FAMILY |
|---|---|
| Access Control | Media Protection |
| Awareness and Training | Personnel Security |
| Audit and Accountability | Physical Protection |
| Configuration Management | Risk Assessment |
| Identification and Authentication | Security Assessment |
| Incident Response | System and Communications Protection |
| Maintenance | System and Information Integrity |

# Threats to information systems

- Threats to information systems can include
  - purposeful attacks,
  - environmental disruptions,
  - human/machine errors, and
  - structural failures,

- “The results can” result in harm to the national and economic security interests of the United States.

NIST SP 800-30; Guide for Conducting Risk Assessments, ch 1, pg 1

# Attack Vectors – broad view

- External/Removable Media:
  - An attack executed from removable media (e.g., flash drive, CD) or a peripheral device.
- Attrition:
  - An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.
- Web:
  - An attack executed from a website or web-based application.
- Email:
  - An attack executed via an email message or attachment.
- Improper Usage:
  - Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.
- Loss or Theft of Equipment:
  - The loss or theft of a computing device or media used by the organization, such as a laptop or smartphone.
- Other:
  - An attack that does not fit into any of the other categories.

NIST SP 800-61 r2; Computer Security Incident Handling Guide, page 2

# Risk Matrix – Cyber Incident

| Business Risk | Likelihood | Likely Impact | Plan |
|---|---|---|---|
| 3rd Party - Asset | Medium | High | Yes |
| Cloud issues | Low | Medium | No |
| Data/Information Sharing | High | High | Yes |
| Forensic Procedures | HIgh | Medium | No |
| Unsecured Information | Low | Medium | Yes |
| Updates | Medium | Medium - High | Yes |
| | | | |

# Cyber Incident

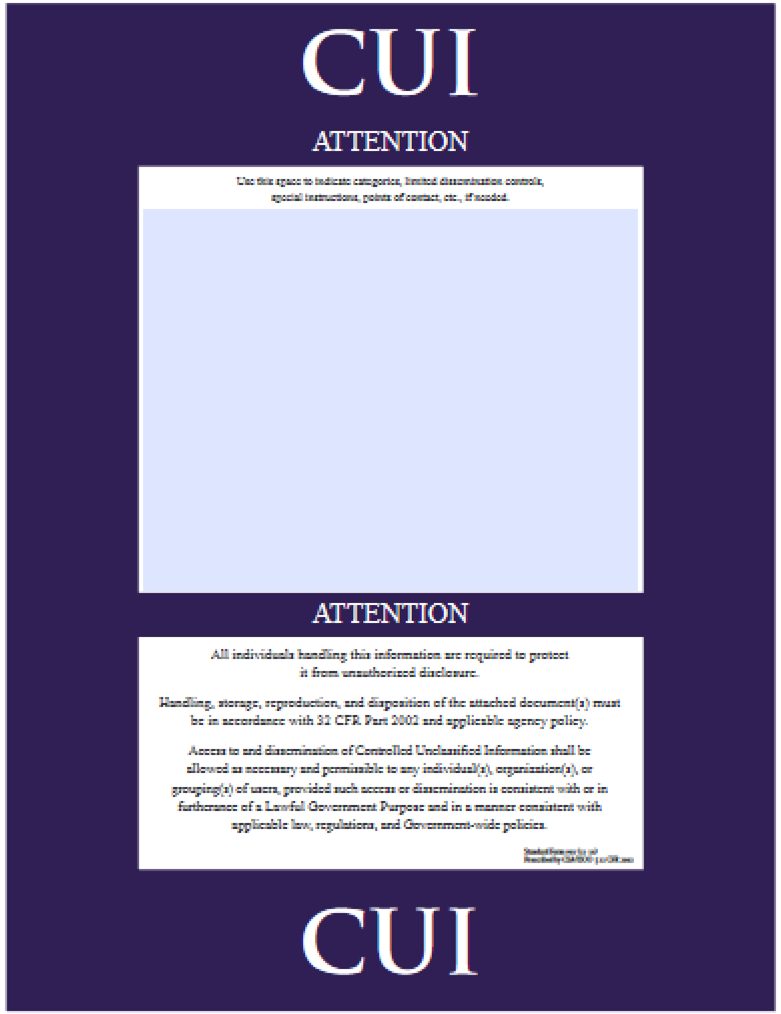
- What does your plan require?, What do the regulations require?
- Who will do what? Who is in charge?
- Who should we contact – for support?
- Have we created a forensic image? What software was used? How do we secure it?
- What other reporting requirements do we have? – legal – IT company - customer – state – local – insurance
- Who has the numbers? What do we say?
- What laws and regulations do we have to comply with to complete the investigation?
- Does the information involved (at risk) fall under any other program? Which programs? ITAR/JCP/Other

# Cyber Incident continued

- What information needs to be collected for reporting to DoD?
- When does the clock start? – the report is due in 72 hours. Who is doing that?
- Who has the Medium Assurance Security Certificate? Can we access it? Is it on an infected machine?
- Do we know how to use it? Do we have an account?
- These are very rough ideas. However, as you can see, a exercise requires active involvement rather than passive listening. It also requires and test knowledge of formal requirements, company procedures and actions to take.
- The above may be one scenario. A follow on scenario may be – the network has crashed and the reports have been made what do we do next – how do we recover?
- An alternative scenario may deal with the impact of shop operations. The company is cold and dark. The machines are silent. A delivery is due. A time sensitive shipment is due to go out later in the day or next week.
- A piece of scrap is found in a recycling bin; the part was nearly complete when the flaw occurred – is this an issue – why?

# Sharing information

- Folder with a CUI coversheet
- Questions –
  - Are all members of our supply chain eligible to receive this information?
  - What issues need to be considered?
  - Do we know we can share with them or do we hope that we can?
  - What type of program do they have?
  - When was the last time we visited/talked and checked/verified?



CUI

ATTENTION

Use this space to indicate categories, limited dissemination controls, special instructions, points of contact, etc., if needed.

ATTENTION

All individuals handling this information are required to protect it from unauthorized disclosure.

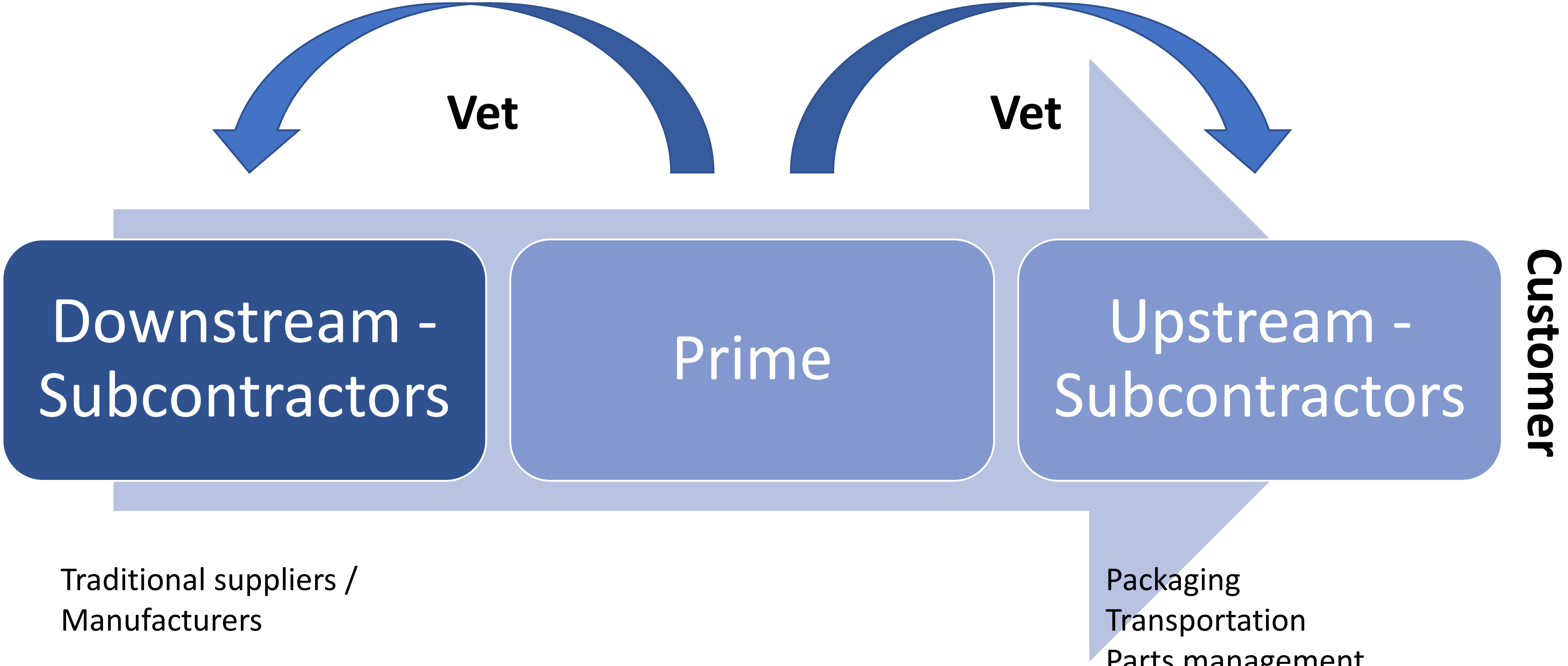
Handling, storage, reproduction, and disposition of the attached document(s) must be in accordance with 32 CFR Part 2002 and applicable agency policy.

Access to and dissemination of Controlled Unclassified Information shall be allowed as necessary and permissible to any individual(s), organization(s), or grouping(s) of users, provided such access or dissemination is consistent with or in furtherance of a Lawful Government Purpose and in a manner consistent with applicable law, regulations, and Government-wide policies.

Standard Form 901 (11-18)
Prescribed by GSA/ISOO | 32 CFR 2002

CUI

# Performance Chain



Vet

Vet

Downstream - Subcontractors

Prime

Upstream - Subcontractors

Customer

Traditional suppliers /
Manufacturers

Packaging
Transportation
Parts management

# CUI Sharing – Discussion Points

- **Determination of eligibility to receive CUI**
- Sharing U.S. Government information with outside entities may only occur if:
  - The entity is authorized to receive the information.
  - The sharer is authorized to pass the information.
  - The sharing complies with U.S. laws and regulations.
  - The sharing benefits the U.S. Government.

CUI Awareness and Marking, November 2020; slide 10

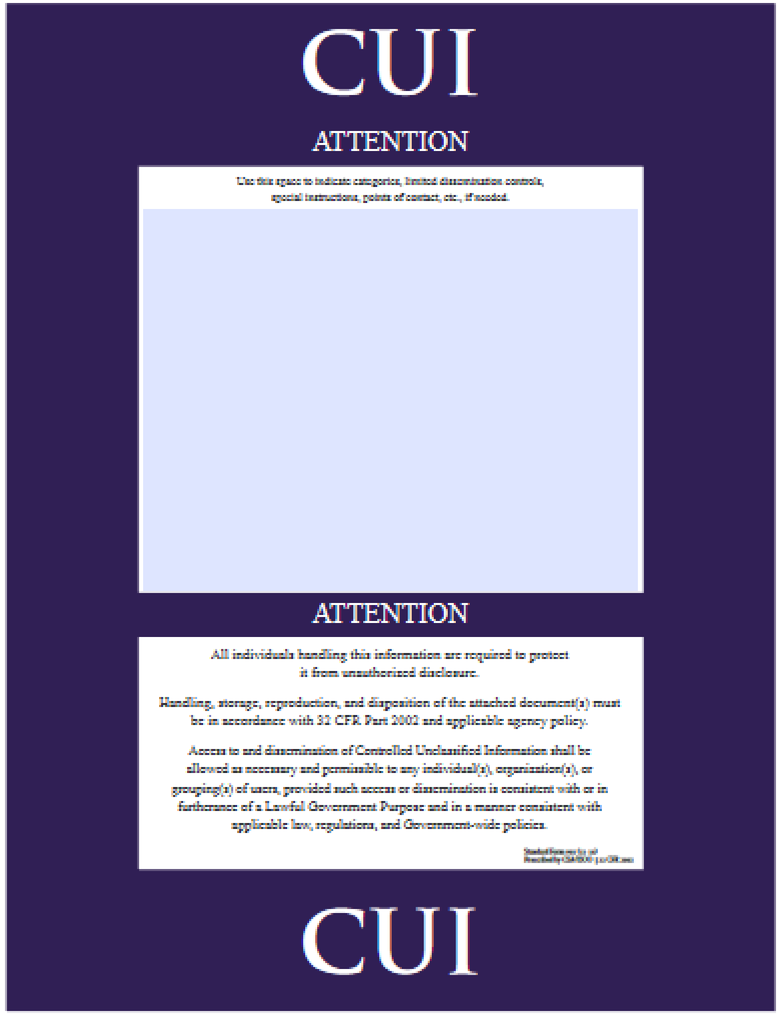
# Create “injects” – “throw a curve-ball”

- **Determination of eligibility to receive CUI**
  - In addition to being CUI, the information is ITAR
  - The company was sold – acquired
    - Is the company eligible – U.S. Person?
    - Is the recipient eligible – U.S. Person?
  - The information is JCP but the proposed recipient is not listed in DLA registry

CUI Awareness and Marking, November 2020; slide 10

# Unattended information

- Folder with a CUI coversheet left unattended in the conference room
- Questions –
    - Is this an issue?
    - What steps should be taken?
    - Who should be involved?
    - Is this a reportable incident?
    - What would make it a reportable incident?
    - What plan/policy changes should be considered?



CUI

ATTENTION

Use this space to indicate categories, limited dissemination controls,
special instructions, points of contact, etc., if needed.

ATTENTION

All individuals handling this information are required to protect
it from unauthorized disclosure.

Handling, storage, reproduction, and disposition of the attached document(s) must
be in accordance with 32 CFR Part 2002 and applicable agency policy.

Access to and dissemination of Controlled Unclassified Information shall be
allowed as necessary and permissible to any individual(s), organization(s), or
grouping(s) of users, provided such access or dissemination is consistent with or in
furtherance of a Lawful Government Purpose and in a manner consistent with
applicable law, regulations, and Government-wide policies.

Standard Form 901 (11-18)
Prescribed by GSA/ISOO | 32 CFR 2002

CUI

# Exercises – help with identifying

How do you measure up?

**Requirements**

Regulations

Laws

**Company**

Practices

Procedures

Policies

# Exercise Development/Selection

## What is the goal?

## What do you want to test?

Knowledge of Plan

Knowledge of systems, devices and equipment

Functionality of system and devices

Response to triggering event

- Immediate (primary)
- Alternate
- Communication
- Coordination

# Dimensions to test

- Hardware
- Software
- Communications
- Physical
- Personal
- Administrative procedural safeguards

- "Software safeguards alone are not sufficient"

Official website of the Department of Homeland Security

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

## 5 Questions CEOs Should Ask About Cyber Risks

1) How Is Our Executive Leadership Informed About the Current Level and Business Impact of Cyber Risks to Our Company?
2) What Is the Current Level and Business Impact of Cyber Risks to Our Company? What Is Our Plan to Address Identified Risks?
3) How Does Our Cybersecurity Program Apply Industry Standards and Best Practices?
4) How Many and What Types of Cyber Incidents Do We Detect In a Normal Week? What is the Threshold for Notifying Our Executive Leadership?
5) How Comprehensive Is Our Cyber Incident Response Plan? How Often Is It Tested?

Where to start

# What to test?

- DFARS 252.204-7012
  - SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEC 2019)
    - Safeguarding
    - Cyber Incident Reporting
  - What is required to Safeguard?
    - Adequate Security
    - NIST 800-171 r2
  - What entails Cyber Incident Reporting
    - (1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall—
    - (i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and
    - (ii) Rapidly report cyber incidents to DoD at https://dibnet.dod.mil.

1. Safeguard
2. Cyber Incident Report

# Integrate terms into the response plan

- “Cyber incident” means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.
- “Compromise” means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

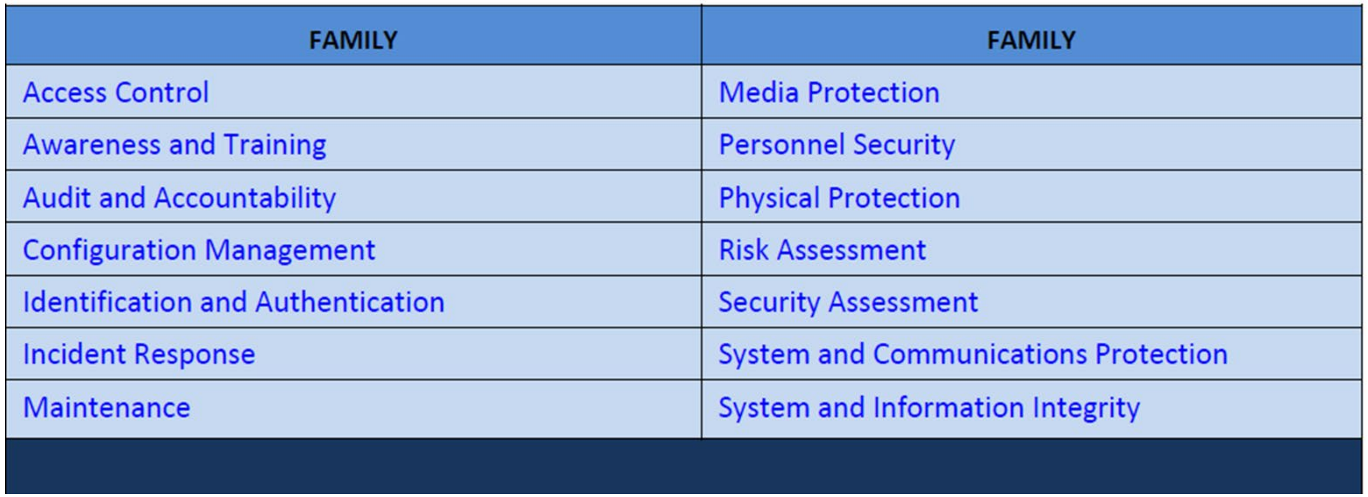
***“Disclosure or Violation”***

Goal/purpose [monitor, detect] is to prevent / identify

DFARS 252.204-7012

# Reframe the question

- How can CUI “escape” the controlled environment?
- What actions result in “disclosure of information to unauthorized persons?”
- Possible pathways



| FAMILY | FAMILY |
|---|---|
| Access Control | Media Protection |
| Awareness and Training | Personnel Security |
| Audit and Accountability | Physical Protection |
| Configuration Management | Risk Assessment |
| Identification and Authentication | Security Assessment |
| Incident Response | System and Communications Protection |
| Maintenance | System and Information Integrity |

# ID Requirements DFARS 252.204-7012 - 1

(c) *Cyber incident reporting requirement*.

(d) *Malicious software.*

(e) *Media preservation and protection*.

(f) *Access to additional information or equipment necessary for forensic analysis.*

(g) *Cyber incident damage assessment activities*.

(h) *DoD safeguarding and use of contractor attributional/proprietary information.*

(i) *Use and release of contractor attributional/proprietary information not created by or for DoD.*

# Incorporate all requirements

- (e) *Media preservation and protection*. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.
- (f) *Access to additional information or equipment necessary for forensic analysis.*Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.
- (g) *Cyber incident damage assessment activities*. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

# Exercise outcomes

- Evaluate the preparedness program
- Identify planning and procedural deficiencies
- Test or validate recently changed procedures or plans
- Clarify roles and responsibilities
- Obtain participant feedback and recommendations for program improvement
- Measure improvement compared to performance objectives
- Improve coordination between internal and external teams, organizations and entities
- Validate training and education
- Increase awareness and understanding of hazards and the potential impacts of hazards.
- Assess the capabilities of existing resources and identify needed resources

https://www.ready.gov/exercises

# Incident data collection

–Status change date/timestamps(including timezone):when the incident started, when the incident was discovered/detected, when the incident was reported, when the incident was resolved/ended, etc.

–Physical location of the incident (e.g., city, state)

–Current status of the incident (e.g., ongoing attack)

–Source/cause of the incident (if known), including hostnames and IP addresses–Description of the incident (e.g., how it was detected, what occurred)

–Description of affected resources (e.g., networks, hosts, applications, data), including systems' hostnames, IP addresses, and function

–If known, incident category, vectors of attack associated with theincident, and indicators related to the incident (traffic patterns, registry keys, etc.)

–Prioritization factors (functional impact, information impact, recoverability, etc.)

–Mitigating factors(e.g., stolen laptop containing sensitive data was using full disk encryption)

–Response actions performed (e.g., shut off host, disconnected host from network)

–Other organizations contacted (e.g., software vendor)

NIST SP 800-61 COMPUTER SECURITY INCIDENT HANDLING GUIDE, pg 58

# What is to be exercised?

- What is to be exercised?
  - Need to be specific.
  - Just saying we will be conducting a cyber security exercise is too broad a statement.
  - What type of exercise will be conducted?
    - Orientation/Walkthrough
    - Table-top
    - Functional
    - Full Scale

# Who will develop the exercise?

Staff

External source – consultant/cyber security firm

Blend – staff & external source

Download Purchase framework / template

# Exercise scope – focus on the 5W's

- (Who, What, Why, Where, When)
- Who are the – Participants
- What is the format (Type) – Table-top, functional, other
- Why is this Exercise being conducted? – test plan
- Where will the drill be located? – Location; conference room, breakroom, live
- When – Duration, Date

# Exercise scope – focus on the 5W's

- Who are the – Participants
  - Pre-constructed emails approved by < company approval> will be sent to the following individuals (shop, procurement, proposal team).
- What is the format (Type) – Table-top, hands-on, other
  - The format is hands-on. Pre-constructed emails will be sent to employee accounts. A designated and briefed facilitatory will observe the response actions.
- Why is this Exercise being conducted?
  1. Ensure staff members handle CUI in accordance with company policies/procedures.
  2. Identify any omissions or inaccuracies in company policies/procedures
- Where will the drill be located? – Location; conference room, breakroom, live
  - The exercise will be conducted online with facilitators/monitors
- When – Duration, Date
  - The exercise is scheduled for <date between xx and xx>

# Create SMART Objectives

- Specific
- Measurable
  - Numeric
  - Descriptive
- Achievable
- Relevant
  - Related to mission / requirements
- Time-bound
  - Within xxxx amount of time
  - Before taking the next action

# Exercise Objective(s)

- Test knowledge of company’s policies, procedures and practices
- Test the correctness of these documents
- Evaluate training
- Identify gaps – weaknesses
- Develop Lessons Learned
- Create Corrective Action Plan
  - Identify item
  - Assign POC
  - Establish time frame

# Determine what is to be tested?

**Effectiveness of Plans, Policies and Practices**

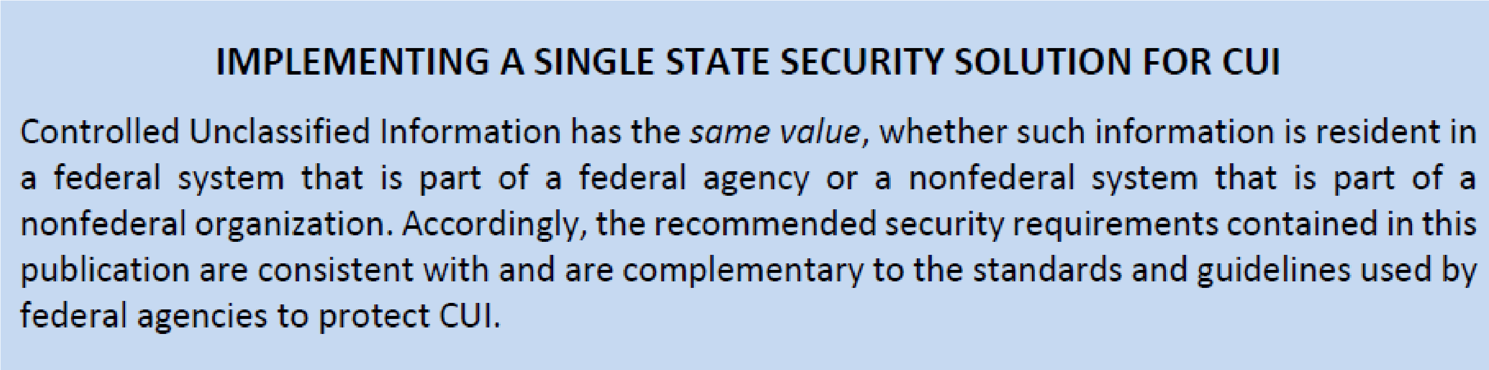
- Identification
- Initial actions/response
- Initial Alert/Communications
- Forensic Evidence Collection
- External Coordination
- External Response
- Recovery
- Data Back up

# How will the exercise be conducted?

- How will performance be measured?
- Are their checklists?
- Are staff members identified?
- Are observers trained?
- Have observers been briefed?
- Is there a facilitator’s guide?
- Is there a participant’s guide?
- Are there evaluation forms?

# One exercise scenario is not enought

- Identify threats (internal & external)
- Identify pathways (communications (email, conversations), visitors, sales, etc.)
- Identify – determine risk / impact
- Rank likelihood



**IMPLEMENTING A SINGLE STATE SECURITY SOLUTION FOR CUI**

Controlled Unclassified Information has the *same value*, whether such information is resident in a federal system that is part of a federal agency or a nonfederal system that is part of a nonfederal organization. Accordingly, the recommended security requirements contained in this publication are consistent with and are complementary to the standards and guidelines used by federal agencies to protect CUI.

# Exchange of Information

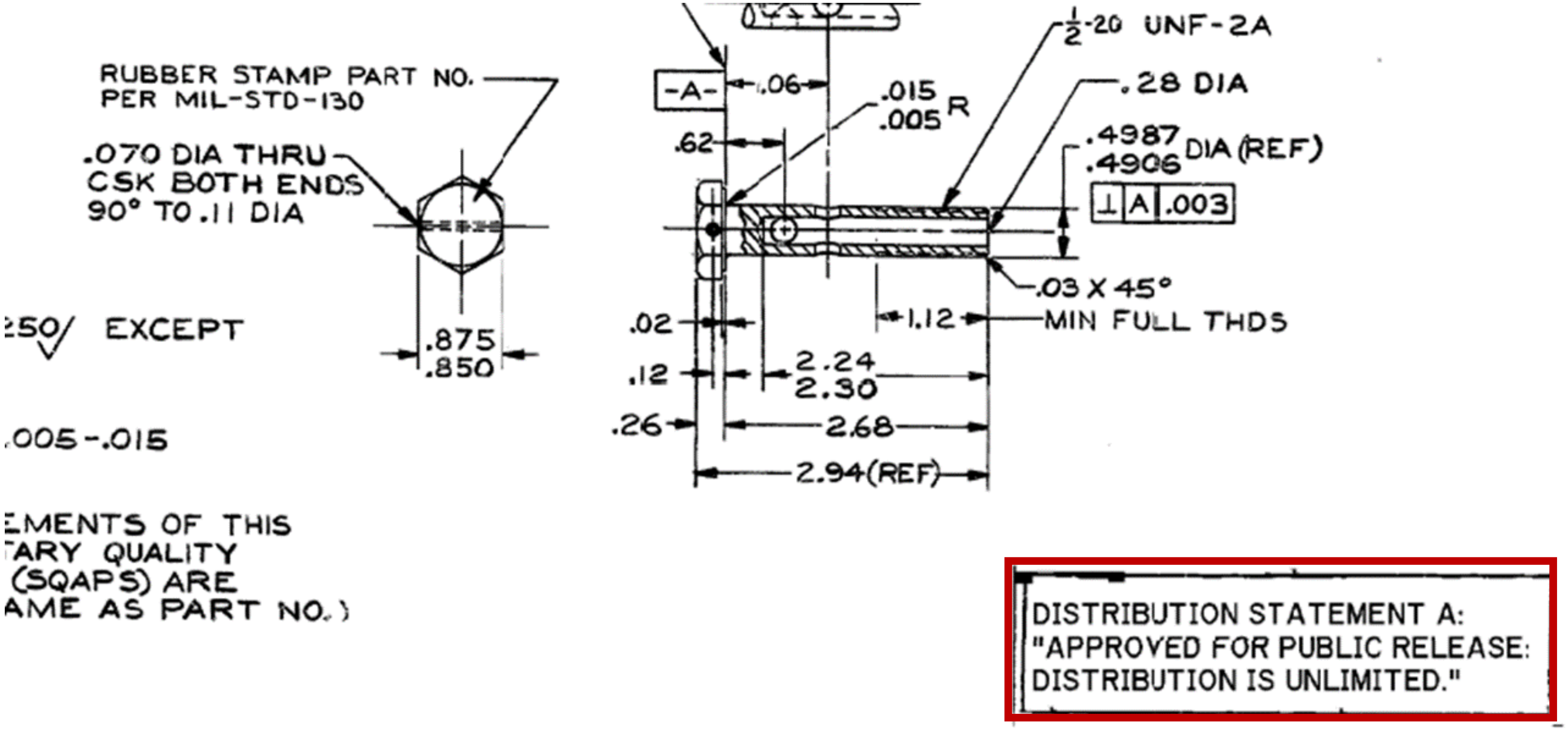
- Non-disclosure agreement (NDA)
- Service Level agreement (SLA)
- Business Partner Connectivity Agreement (BPCA)
- DFARS 252.204-7012 Reporting Requirements – prime/sub
- Others agreements as required and allowed
    - Lawful governmental purpose v. Business purpose
- Thoroughly vetted and authorized by law, regulation or other authority
- DoD contractors – don’t overlook DFARS 252.204-7000

# Scenario – data export

- **General scenario**: A staff member receives an email requesting that they forward specific contract information to a potential subcontractor. The POC's contact information (phone and email) is provided.

# Distribution Statement A - example

Testing familiarity with Distribution Statements



DISTRIBUTION STATEMENT A:
"APPROVED FOR PUBLIC RELEASE:
DISTRIBUTION IS UNLIMITED."

Attachment to client email

# Incident Handling Scenarios

- Incident handling scenarios provide an inexpensive and effective way to build incident response skills and identify potential issues with incident response processes.
- The incident response team or team members are presented with a scenario and a list of related questions.
- The goal is to determine what the team would really do and to compare that with policies, procedures, and generally recommended practices to identify discrepancies or deficiencies.

NIST SP 800-61 COMPUTER SECURITY INCIDENT HANDLING GUIDE, pg 52

# Now what? – re: Ransomware

- Is there a plan?
- Online, accessible?
- Printed?
- Does it work?
- Who do you call?
- Do you have the numbers?
- Are there any support/response agreements – time specified?
- Lawyer, Law enforcement, Insurance, 3rd Party IT, Cyber