Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

Cyber Friday

Incident Identification, Reporting Requirements, and Recovery

November 18, 2022




Webinar Etiquette

PLEASE

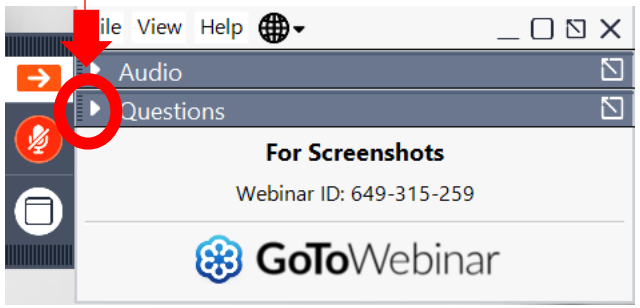
- Log into the GoToWebinar session with the name that you registered with online
- Place your phone or computer on MUTE
- Use the QUESTIONS option to ask your question(s).
  - We will share the questions with our guest speaker who will respond to the group

THANK YOU!

QUESTIONS?

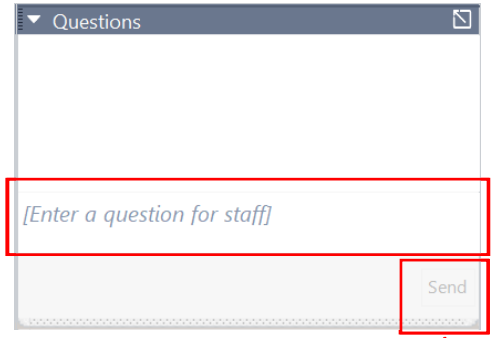
OPENING THE QUESTIONS BOX

Click here to access
within the Control Panel



USING THE QUESTIONS BOX

Type questions
here at any time
during a
presentation



Click Send when ready to submit a question

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
Cyber Friday

ABOUT WPI
Supporting the mission

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
Cyber Friday

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

Assist businesses in creating, developing and growing their sales, revenue and jobs through Federal, State and Local Government contracts.

- **INDIVIDUAL COUNSELING – At our offices, at client's facility or via telephone/GoToMeeting**
- **SMALL GROUP TRAINING – Workshops and webinars**
- **CONFERENCES to include one on one or roundtable sessions**

Last year WPI provided training at over 100 events and provided service to over 1,200 companies

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
Cyber Friday

WPI is a Procurement Technical Assistance Center (PTAC) funded in part by the Department of Defense (DOD), WEDC and other funding sources.

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

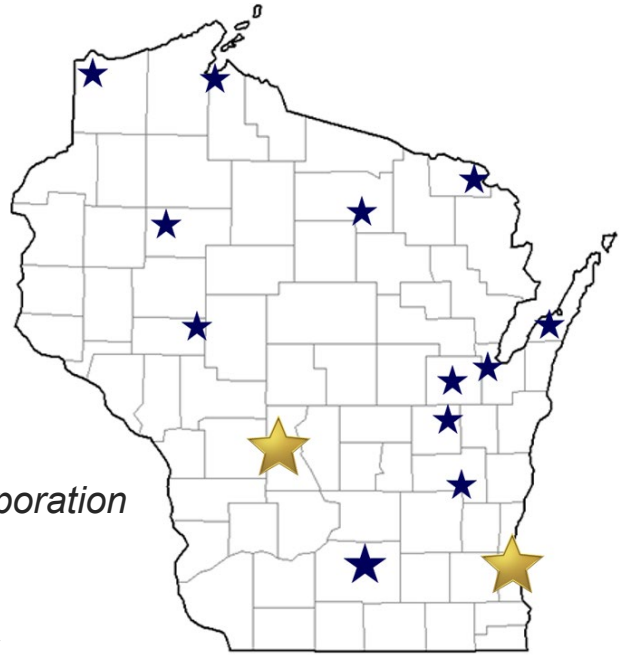
Sign-up for our Newsletter

Stay up-to-date with the latest WPI news and events.

https://www.wispro.org/newsletter-signup/

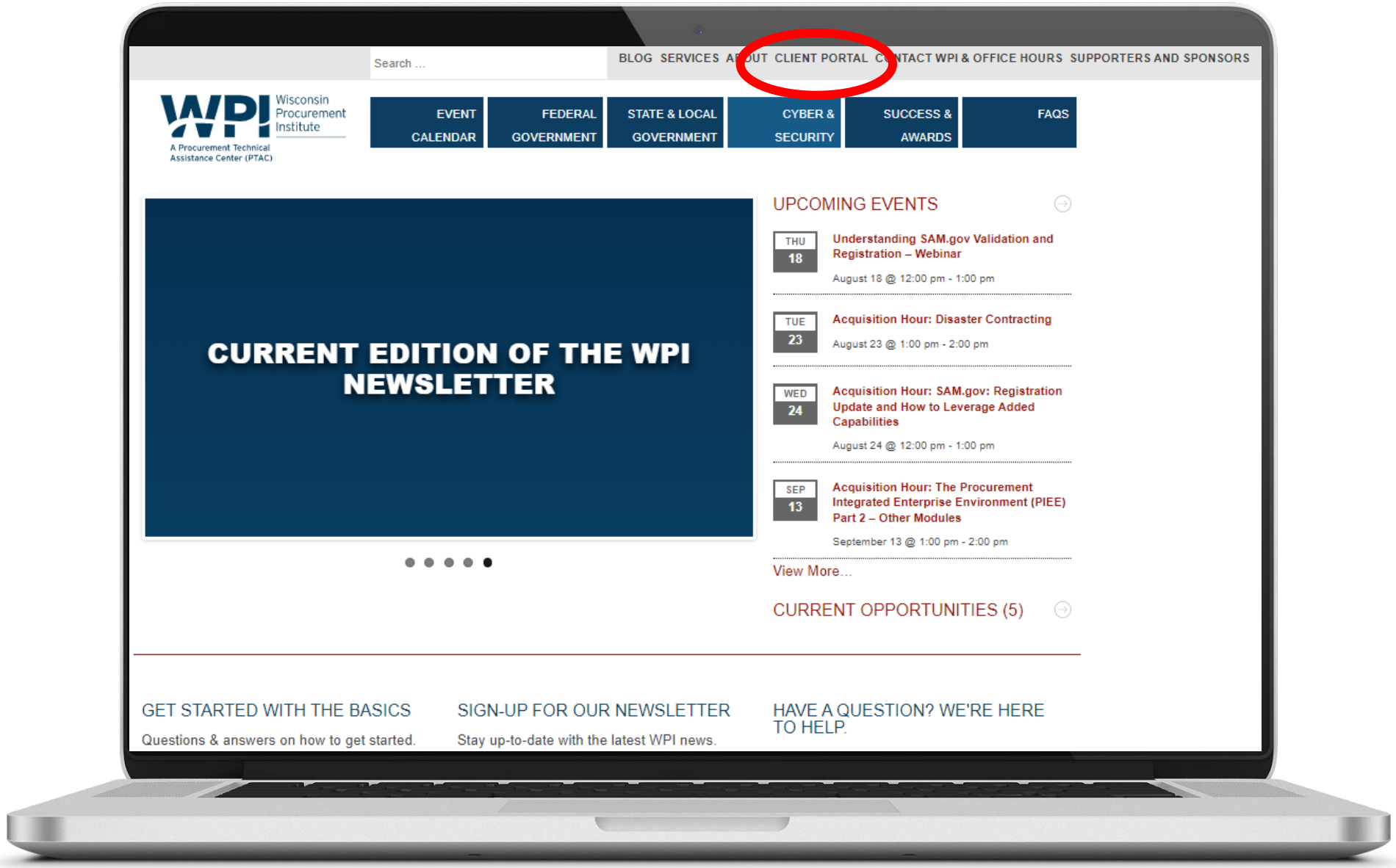
WPI OFFICE LOCATIONS

- **MILWAUKEE**
  - *Technology Innovation Center*
- **MADISON**
  - *FEED Kitchens*
  - *Dane County Latino Chamber of Commerce*
  - *Wisconsin Manufacturing Extension Partnership (WMEP)*
  - *Madison Area Technical College (MATC)*
- **CAMP DOUGLAS**
  - *Juneau County Economic Development Corporation (JCEDC)*
- **FOND DU LAC**
  - *Envision Greater Fond du Lac*
- **GREEN BAY**
  - *NWTC Startup Hub*
- **APPLETON**
  - *Fox Valley Technical College*
- **OSHKOSH**
  - *Fox Valley Technical College*
  - *Greater Oshkosh Economic Development Corporation*
- **EAU CLAIRE**
  - *Western Dairyland*
- **LADYSMITH**
  - *Indianhead Community Action Agency*
- **RHINELANDER**
  - *Nicolet Area Technical College*
- **ASHLAND**
  - *Ashland Area Development Corporation*
- **FLORENCE**
  - *Florence County Economic Development*
- **DOOR COUNTY**
  - *NE WI Technical College*
  - *Door County Economic Development Corporation*
- **SUPERIOR**
  - *Small Business Dev Center; UW Superior*



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

Cyber Friday


Search ...
BLOG SERVICES ABOUT CLIENT PORTAL CONTACT WPI & OFFICE HOURS SUPPORTERS AND SPONSORS
WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
EVENT CALENDAR
FEDERAL GOVERNMENT
STATE & LOCAL GOVERNMENT
CYBER & SECURITY
SUCCESS & AWARDS
FAQS
CURRENT EDITION OF THE WPI NEWSLETTER
UPCOMING EVENTS
THU 18
Understanding SAM.gov Validation and Registration – Webinar
August 18 @ 12:00 pm - 1:00 pm
TUE 23
Acquisition Hour: Disaster Contracting
August 23 @ 1:00 pm - 2:00 pm
WED 24
Acquisition Hour: SAM.gov: Registration Update and How to Leverage Added Capabilities
August 24 @ 12:00 pm - 1:00 pm
SEP 13
Acquisition Hour: The Procurement Integrated Enterprise Environment (PIEE) Part 2 – Other Modules
September 13 @ 1:00 pm - 2:00 pm
View More...
CURRENT OPPORTUNITIES (5)
GET STARTED WITH THE BASICS
Questions & answers on how to get started.
SIGN-UP FOR OUR NEWSLETTER
Stay up-to-date with the latest WPI news.
HAVE A QUESTION? WE'RE HERE TO HELP.

Incident Identification, Reporting Requirements, and Recovery

Marc N. Violante

Wisconsin Procurement Institute

November 18, 2022

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

Webinar Description

- Both FAR 52.204-21 and DFARS 252.204-7012 require companies to report cyber incidents. In addition, DFARS 252.204-7012 requires companies to implement NIST 800-171 r2 and to formally investigate the incident, preserve forensic evidence, and be prepared to support additional information requires from DoD. Additionally, Section 3.6 of NIST 800-171 r2 requires companies to, “Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.” This webinar will review these requirements, references, resources, and actions that companies can use to develop their plans.

$$\text{Cybersecurity} = \text{SSP} + \text{POA\&M}$$

Cybersecurity – general focus

Why does it matter

- **Iranian Hackers Compromised a Federal Agency's Network, CISA and FBI Say**
- CISA and the FBI said the unnamed "federal civilian executive branch organization" was compromised "as early as February 2022."

The breach occurred just months after CISA issued an emergency directive in December 2021, requiring federal agencies to assess their networks for the Log4Shell vulnerability and "immediately patch these systems or implement other appropriate mitigation measures." The directive gave agencies until 5 p.m. on Dec. 23 of that year to identify whether their software was affected by the vulnerability, by using a CISA-managed GitHub repository "to determine whether Log4j is present in those assets and if so, whether those assets are affected by the vulnerability." Agencies were also given a Dec. 28 deadline to report back to CISA on "all affected software," as well as the steps they had taken to address the vulnerability.

https://www.nextgov.com/cybersecurity/2022/11/iranian-hackers-compromised-federal-agencys-network-cisa-and-fbi-say/379832/

Incident - examples

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
- A user provides or exposes sensitive information to others through peer-to-peer file sharing services

NIST SP 800-61 r2; Computer Security Incident Handling Guide, page 6

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

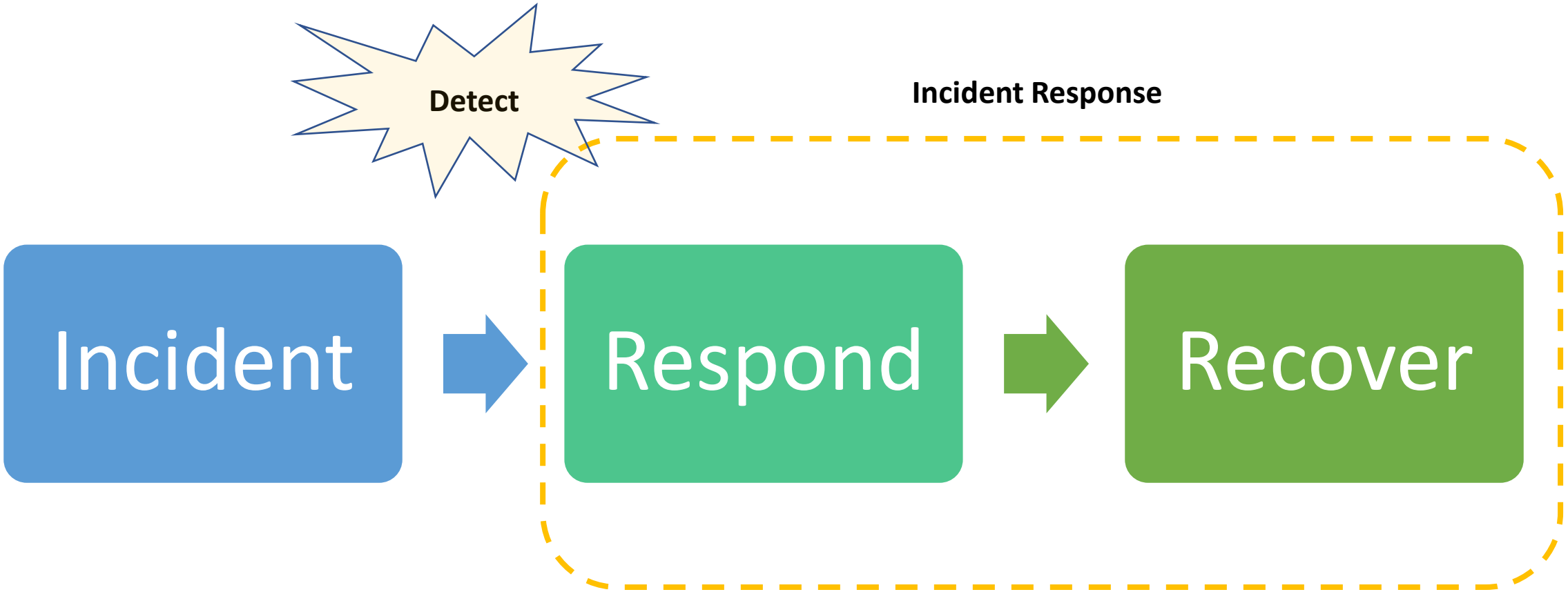
Threats to information systems

- 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

Incident Response



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

Cybersecurity = SSP + POA&M + Incident Response

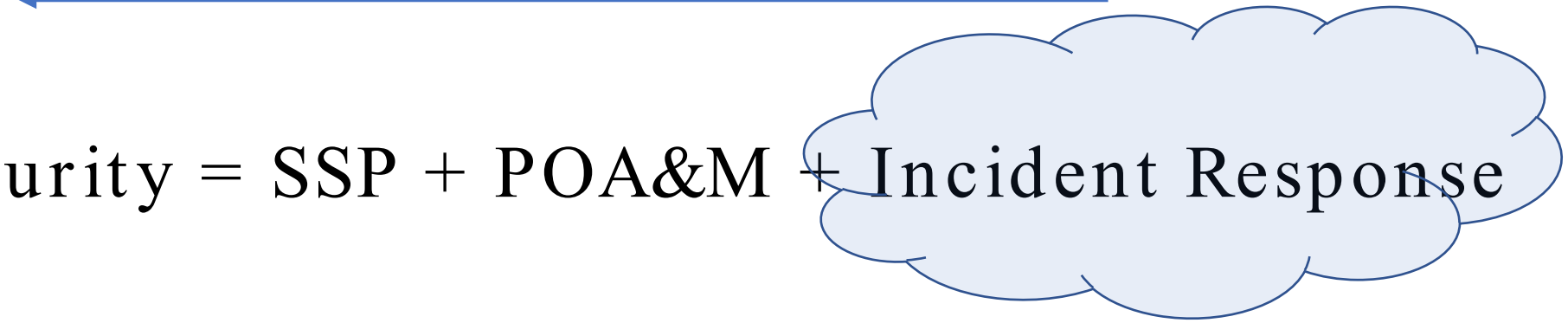
Cybersecurity

Need for Incident Response

- Attacks frequently compromise personal and business data {**DoD CDI **}
- it is critical to respond quickly and effectively when security breaches occur.
- One of the benefits of having an incident response capability is that it supports responding to incidents systematically (i.e., following a consistent incident handling methodology) so
  - the appropriate actions are taken.
- Incident response helps personnel to minimize loss or theft of information and disruption of services caused by incidents.
- Another benefit of incident response is the ability to use information gained during incident handling to better prepare for handling

NIST SP 800-61 r2; Computer Security Incident Handling Guide, page 6

Knowledge, experience, data, findings, suggestions



Cybersecurity

Cyber Threat Sharing

- includes indicators (system artifacts or observables associated with an attack),
- tactics, techniques, and procedures (TTPs),
- security alerts,
- threat intelligence reports, and
- recommended security tool configurations

NIST SP 800-150; GUIDE TO CYBER THREAT INFORMATION SHARING, page iii

Value of Information Sharing

- organizations can leverage
  - the collective knowledge,
  - experience, and
  - capabilities of that sharing community
  - to gain a more complete understanding of the threats the organization may face.

NIST SP 800-150; GUIDE TO CYBER THREAT INFORMATION SHARING, page iii

Establish information sharing rules

- intended to control the publication and distribution of threat information, and consequently, help to prevent the dissemination of information that, if improperly disclosed, may have adverse consequences
    - for an organization,
    - its customers, or
    - its business partners.
- Information sharing rules should take into consideration
    - the trustworthiness of the recipient,
    - the sensitivity of the shared information, and
    - the potential impact of sharing (or not sharing) specific types of information

Communications with Outside Parties

NIST SP 800-61 r2; Computer Security Incident Handling Guide, page 10

Information Handling Considerations

- What information do we have?
- What information do we use?
- With whom is information being shared?
- What information is being shared?
- What are the handling requirements?
- Where – how is the information being shared?
- When – normal hours / off hours
- Why is it being shared?
- Other questions ---

Information types v. handling requirements

CUI	ITAR	JCP	Customer (x) – IP	Corporate – IP
• Lawful Governmental Purpose • DOD Required Training • DFARS 252.204 – 7012 / Basic Assessment, SPRS	• US Person – US Person • Registration • ITAR Compliance Program	• Data Custodian – Data Custodian • SAM, PIEE, DOD Basic Assessment, SPRS, DFARS 252.204-7012		

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

DFARS 252.204-7000

See next slide

Disclosure of Information

As prescribed in 204.404-70 (a), use the following clause:

DISCLOSURE OF INFORMATION (OCT 2016)

(a) The Contractor shall not release to anyone outside the Contractor's organization any unclassified information, regardless of medium (e.g., film, tape, document), pertaining to any part of this contract or any program related to this contract, unless—

(1) The Contracting Officer has given prior written approval;

(2) The information is otherwise in the public domain before the date of release; or

(3) The information results from or arises during the performance of a project that involves no covered defense information (as defined in the clause at DFARS 252.204-7012) and has been scoped and negotiated by the contracting activity with the contractor and research performer and determined in writing by the contracting officer to be fundamental research (which by definition cannot involve any covered defense information), in accordance with National Security Decision Directive 189, National Policy on the Transfer of Scientific, Technical and Engineering Information, in effect on the date of contract award and the Under Secretary of Defense (Acquisition, Technology, and Logistics) memoranda on Fundamental Research, dated May 24, 2010, and on Contracted Fundamental Research, dated June 26, 2008 (available at DFARS PGI 204.4).

(b) Requests for approval under paragraph (a)(1) shall identify the specific information to be released, the medium to be used, and the purpose for the release. The Contractor shall submit its request to the Contracting Officer at least 10 business days before the proposed date for release.

(c) The Contractor agrees to include a similar requirement, including this paragraph (c), in each subcontract under this contract. Subcontractors shall submit requests for authorization to release through the prime contractor to the Contracting Officer.

(End of clause)

DFARS 252.204-7000 – partial & reformatted

DISCLOSURE OF INFORMATION (OCT 2016)

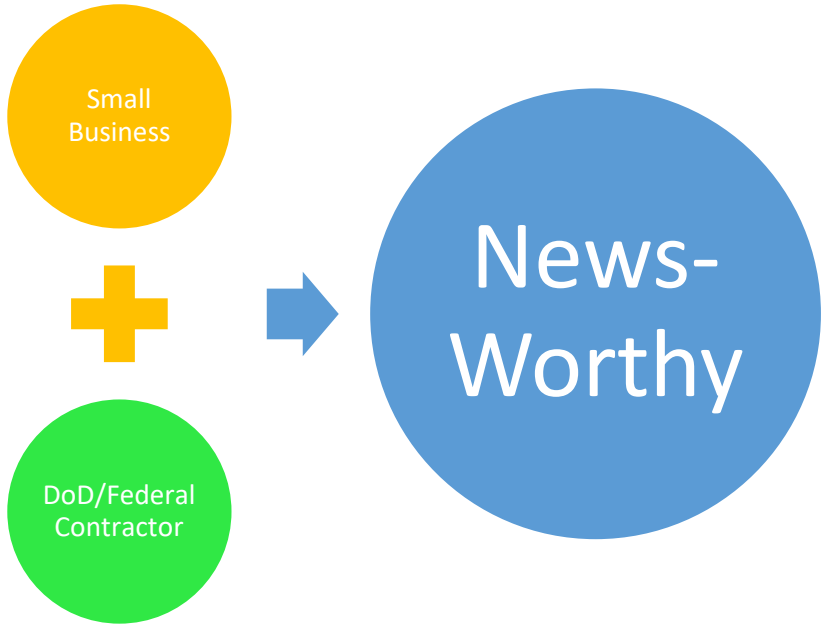
(a) The Contractor

- shall not release to anyone outside the Contractor's organization
- any unclassified information,
- regardless of medium (e.g., film, tape, document),
- pertaining to any part of this contract or any program related to this contract,

• unless—

(1) The Contracting Officer has given prior written approval;

Communications – the Media



- Conduct training
  - Protect sensitive information
  - Countermeasures / actions
  - Anything that could help the attackers
- Establish policy
- Identify POC

NIST SP 800-61 r2; Computer Security Incident Handling Guide, page 6

Access to CUI

(1) No individual may have access to CUI information unless it is determined he or she has an authorized, lawful government purpose.

(2) The person with authorized possession, knowledge, or control of CUI will determine whether an individual has an authorized, lawful government purpose to access designated CUI.

(3) CUI information may be disseminated within the DoD Components and between DoD Component officials and DoD contractors, consultants, and grantees to conduct official business for the DoD, provided dissemination is consistent with controls imposed by a distribution statement or limited dissemination controls (LDC).

DoDI 5200.48, March 6, 2020; pgs 19-20

Handling of information

- The authorized holder of a document or material is responsible for determining, at the time of creation, whether information in a document or material falls into a CUI category.
- If so, the authorized holder is responsible for applying CUI markings and dissemination instructions accordingly.

DoDI 5200.48, March 6, 2020; pg 17

Security Protection Asset Examples

Asset Type	Security Protection Asset Examples
People	• Consultants who provide cybersecurity service • Managed service provider personnel who perform system maintenance • Enterprise network administrators
Technology	• Cloud-based security solutions • Hosted Virtual Private Network (VPN) services • SIEM solutions
Facility	• Co-located data centers • Security Operations Centers (SOCs) • Contractor office buildings

CMMC Assessment Scope – Level 2 | Version 2.0; page 4

Specialized Assets

- **Government Property** is all property owned or leased by the government. Government property includes both government-furnished and contractor-acquired property. Government property includes material, equipment, special tooling, special test equipment, and real property. Government property does not include intellectual property or software [Reference: Federal Acquisition Regulation (FAR) 52.245-1].
- **IoT or Industrial Internet of Things (IIoT)** are interconnected devices having physical or virtual representation in the digital world, sensing/actuation capability, and programmability features. They are uniquely identifiable and may include smart electric grids, lighting, heating, air conditioning, and fire and smoke detectors [Reference: iot.ieee.org/definition; National Institute of Standards and Technology (NIST) 800-183].
- **OT**[1] is used in manufacturing systems, industrial control systems (ICS), or supervisory control and data acquisition (SCADA) systems. OT may include programmable logic controllers (PLCs), computerized numerical control (CNC) devices, machine controllers, fabricators, assemblers, and machining.
- **Restricted Information Systems** can include systems [and associated Information Technology (IT) components comprising the system] that are configured based on government requirements (i.e., connected to something that was required to support a functional requirement) and are used to support a contract (e.g., fielded systems, obsolete systems, and product deliverable replicas).
- **Test Equipment** can include hardware and/or associated IT components used in the testing of products, system components, and contract deliverables (e.g., oscilloscopes, spectrum analyzers, power meters, and special test equipment).

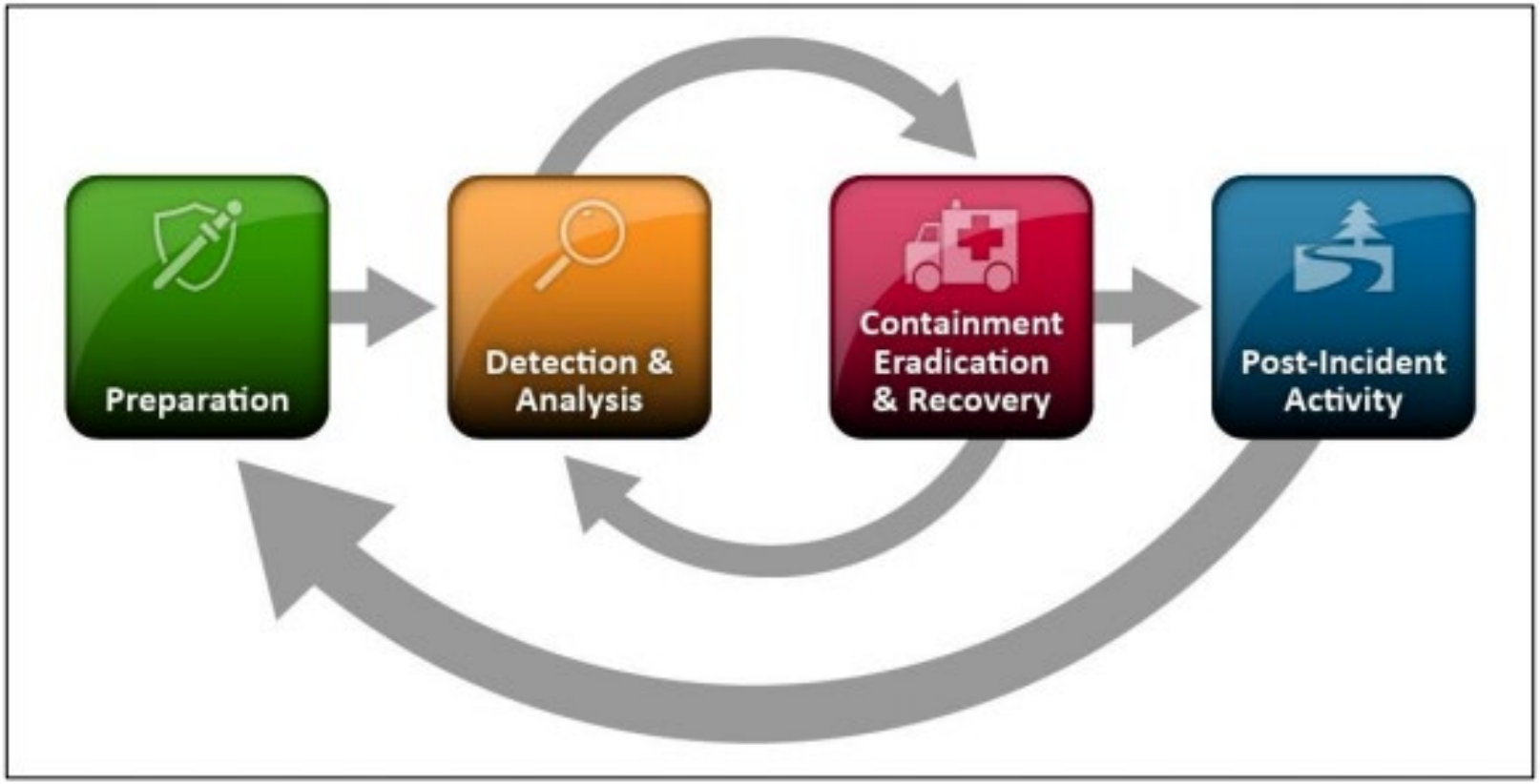
Identifying the CMMC Assessment Scope CMMC Assessment Scope – Level 2 | Version 2.0, page 5

Importance of marking non-government information

(h) *DoD safeguarding and use of contractor attributional/proprietary information.* The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

DFARS 252.204-7012

Incident Response Life Cycle



NIST SP 800-61 r2; Computer Security Incident Handling Guide, Figure 3-1, page 21

Identify & Develop Containment Strategies

- Define acceptable risk
- Understand “one size doesn’t fit all”
  - Develop strategies for various type of incidents
  - Document criteria to facilitate decision making

NIST SP 800-61 r2; Computer Security Incident Handling Guide, page 35

Containment Strategy - criteria

"Isolate"

- Potential damage to and theft of resources
- Need for evidence preservation
- Service availability (e.g., network connectivity, services provided to external parties)
- Time and resources needed to implement the strategy
- Effectiveness of the strategy (e.g., partial containment, full containment)
- Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution).

NIST SP 800-61 r2; Computer Security Incident Handling Guide, page 35

Containment - considerations

- Containment is important before an incident overwhelms resources or increases damage.
- Most incidents require containment, so that is an important consideration early in the course of handling each incident.
- Containment provides time for developing a tailored remediation strategy.
- An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, disable certain functions).

NIST SP 800-61 r2; Computer Security Incident Handling Guide, page 35

Incident Response – Team considerations

- "Create an organization-specific definition of the term "incident" so that the scope of the term is clear."
  - *"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." DFARS - 7012*
- The organization should decide what
  - services the incident response team should provide,
  - consider which team structures and models can provide those services,
  - and select and implement one or more incident response teams.
- Incident response plan, policy, and procedure creation is an important part of establishing a team, so that incident response is performed effectively,

NIST SP 800-61 r2; Computer Security Incident Handling Guide, page 6

Incident Analysis Hardware Software

- **Digital forensic workstations[21] and/or backup devices** to create disk images, preserve log files, and save other relevant incident data
- **Laptops** for activities such as analyzing data, sniffing packets, and writing reports
- **Spare workstations, servers, and networking equipment, or the virtualized equivalents**, which may be used for many purposes, such as restoring backups and trying out malware
- **Blank removable media**
- **Portable printer** to print copies of log files and other evidence from non-networked systems
- **Packet sniffers and protocol analyzers** to capture and analyze network traffic
- **Digital forensic software** to analyze disk images
- **Removable media** with trusted versions of programs to be used to gather evidence from systems
- **Evidence gathering accessories**, including hard-bound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape, to preserve evidence for possible legal actions

NIST SP 800-61 r2; Computer Security Incident Handling Guide, page 22

Outsourcing Considerations

- Current and Future Quality of Work
- Division of Responsibilities
- Sensitive Information Revealed to the Contractor (CUI?)
- Lack of Organization-Specific Knowledge
- Lack of Correlation
- Handling Incidents at Multiple Locations
- Maintaining Incident Response Skills In-House

NIST SP 800-61 r2; Computer Security Incident Handling Guide, page 15

Team Models

- Central Incident Response Team
- Distributed Incident Response Team
- Coordinating Team
- Staffing models
  - Employees
  - Partially Outsourced
  - Fully Outsourced

NIST SP 800-61 r2; Computer Security Incident Handling Guide, pages 13-14

Team Model Selection criterion

- Cost
- Coverage
  - 24-7
  - Part time
  - Employee morale

NIST SP 800-61 r2; Computer Security Incident Handling Guide, page 14

General comparison

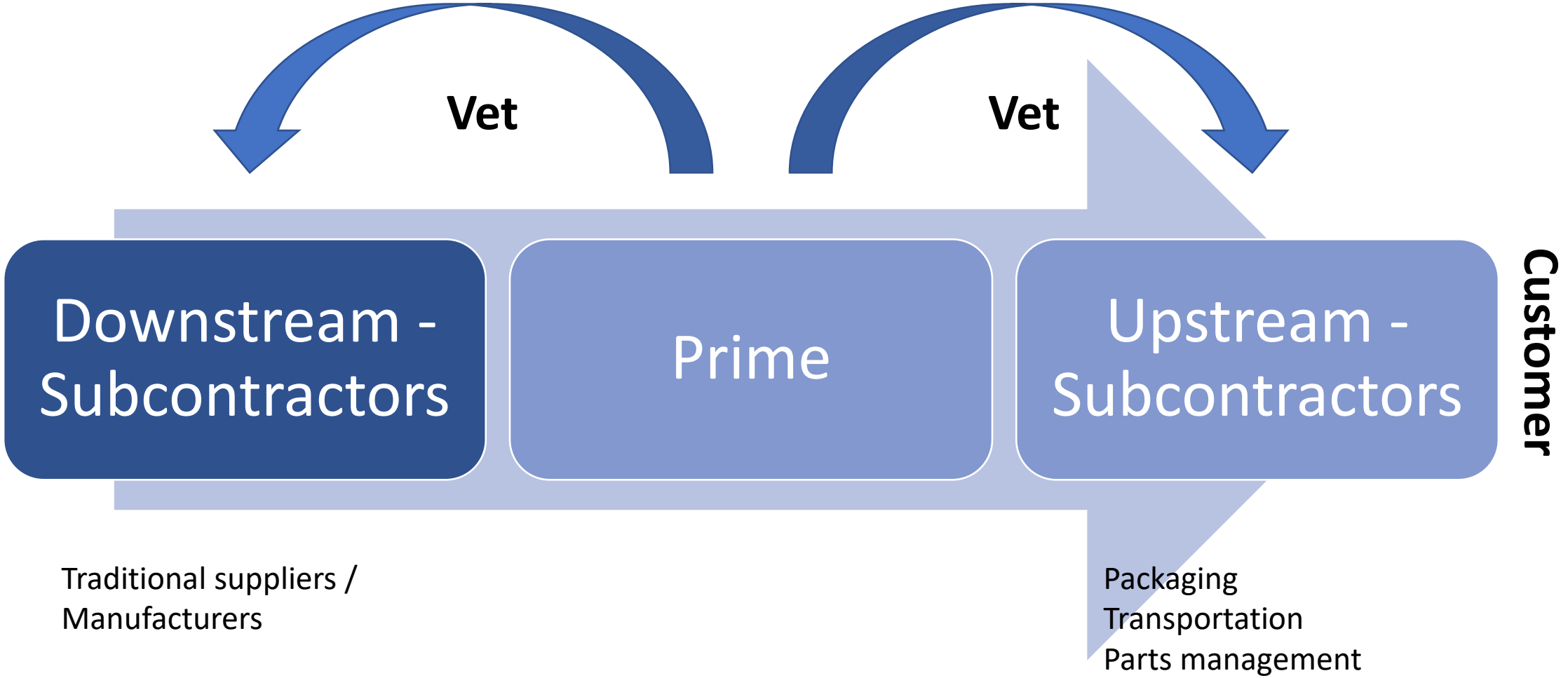
FAR 52.204-21

- FCI
- Does not reference an outside document
- Does not exempt other requirements
- Flowdown – substance of + requiring paragraph

DFARS 252.204-7012

- CUI
- References and requires NIST 800-171 r2
- Does not exempt other requirements
- Flowdown – the clause + requiring paragraph

Performance Chain



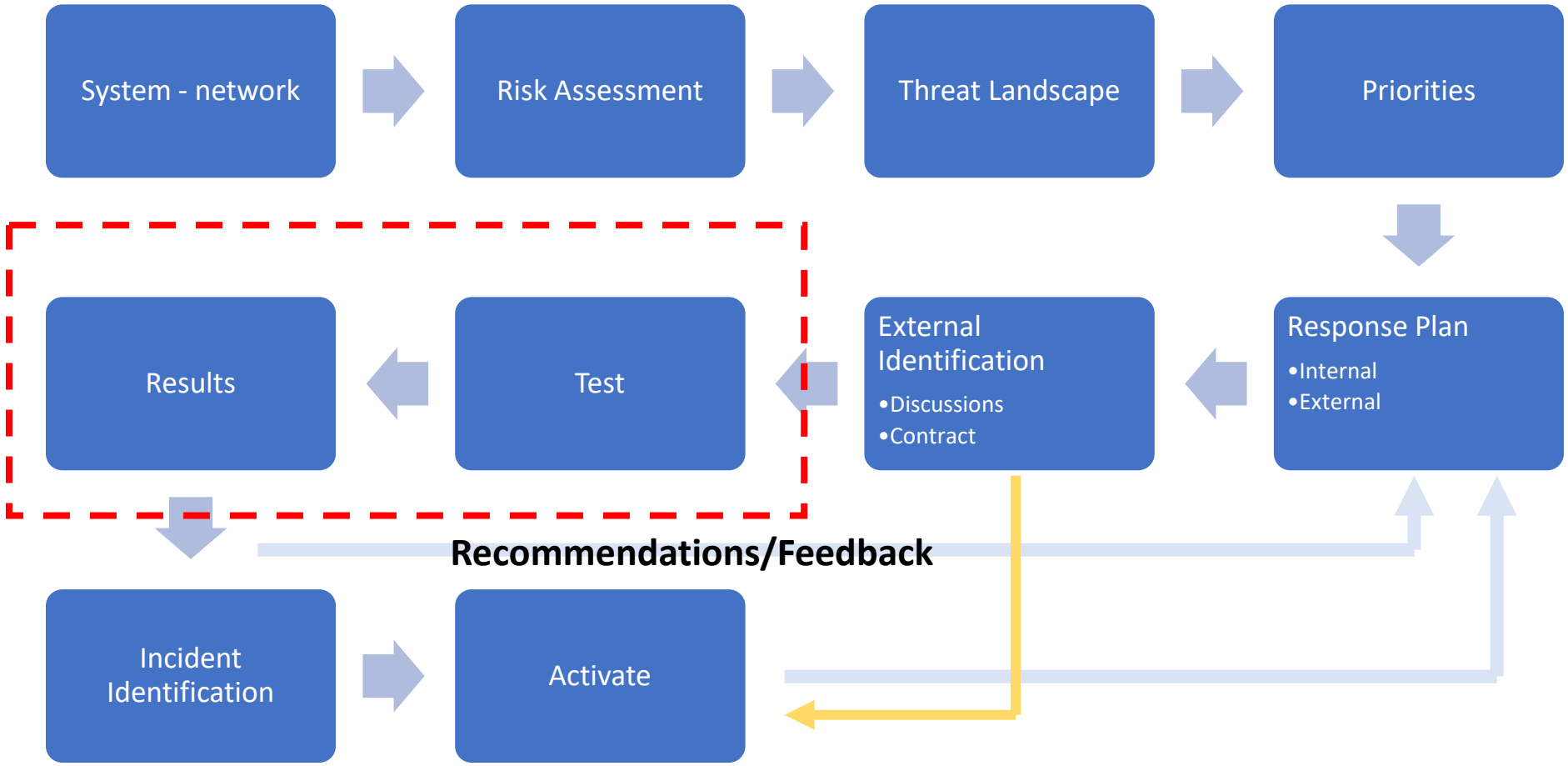
Balance

What requires Incident Response?

Response driven by

- Impact
- Restore
- Required

Cybersecurity Incidents – plan, test, execute



The purpose of risk assessments

- is to inform decision makers and support risk responses by identifying:

  (i) relevant threats to organizations or threats directed through organizations against other organizations;

  (ii) vulnerabilities both internal and external to organizations;

  (iii) impact (i.e., harm) to organizations that may occur given the potential for threats exploiting vulnerabilities; and

  (iv) likelihood that harm will occur. The end result is a determination of risk

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

Organizational risk

- can include many types of risk
  - program management risk,
  - investment risk,
  - budgetary risk,
  - legal liability risk,
  - safety risk,
  - inventory risk,
  - supply chain risk, and
  - security risk). Security risk related to the operation and use of information systems is just one of many components of organizational risk that senior leaders/executives address as part of their ongoing risk management responsibilities.

NIST SP 800-39; Managing Information Security Risk Organization, Mission, and Information System View, Ch 1, pg 1

Plan Elements

- Mission
- Strategies and goals
- Senior management approval
- Organizational approach to incident response
- How the incident response team will communicate with the rest of the organization and with other organizations
- Metrics for measuring the incident response capability and its effectiveness
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization

NIST SP 800-61 r2; Computer Security Incident Handling Guide, page 8

Policy – Organizational structure …

- Organizational structure and definition of roles, responsibilities, and levels of authority; should include the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity, the requirements for reporting certain types of incidents, the *requirements and guidelines for external communications and information sharing* (e.g., what can be shared with whom, when, and over what channels), and the handoff and escalation points in the incident management process

"Authorities | Reporting Requirements | External Communications"

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

Policy Elements

- Statement of management commitment
- Purpose and Objective of the policy
- Scope of the policy (to whom and what it applies and under what circumstances)***
- Definition of computer security incidents and related terms
- Organizational structure and definition of roles, responsibilities, and levels of authority
- **Prioritization or severity ratings of incidents**
- Performance measures
- Reporting and contact forms.

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

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

FAR 52.204-21 – key definitions

- (xii) Identify, report, and correct *information* and *information system* flaws in a timely manner.

- *Information* means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).
- *Information system* means a discrete set of *information* resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of *information* (44 U.S.C. 3502).

FAR 52.204-21 – detailed requirements

- (xii) Identify, report, and correct *information* and *information system* flaws in a timely manner.

  - Identify information flaws in a timely manner
  - Report information flaws in a timely manner
  - Correct information in a timely manner

  - Report information system flaws in a timely manner
  - Identify information system flaws in a timely manner
  - Correct information system flaws in a timely manner

FAR 52.204-21 - questions

- What is to be reported?
- When is it to be reported?
- What format is to be used?
- To whom is it to be reported?
- Are there other requirements?

Identify - Required Information

1. Company name
2. Company point of contact information (address, position, telephone, email)
3. Data Universal Numbering System (DUNS) Number
4. Contract number(s) or other type of agreement affected or potentially affected
5. Contracting Officer or other type of agreement point of contact (address, position, telephone, email)
6. USG Program Manager point of contact (address, position, telephone, email)
7. Contract or other type of agreement clearance level (Unclassified, Confidential, Secret, Top Secret, Not applicable)
8. Facility CAGE code
9. Facility Clearance Level (U, C, S, TS, Not applicable)
10. Impact to Covered Defense Information
11. Ability to provide operationally critical support
12. Date incident discovered
13. Location(s) of compromise
14. Incident location CAGE code
15. DoD programs, platforms or systems involved
16. Type of compromise (unauthorized access, unauthorized release (includes inadvertent release), unknown, not applicable)
17. Description of technique or method used in cyber incident
18. Incident outcome (successful compromise, failed attempt, unknown)
19. Incident/Compromise narrative
20. Any additional information

https://dibnet.dod.mil/portal/intranet/

Identify specific requirements

- “Covered contractor information system” means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.
- “Rapidly report” means within 72 hours of discovery of any cyber incident.
- “Forensic analysis” means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

DFARS 252.204-7012

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.

DFARS Cyber Incident Reporting Requirement

- (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.

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.*

DFARS 252.204-7012-2

(j) *Use and release of contractor attributional/proprietary information created by or for DoD.*

(k) The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(l) *Other safeguarding or reporting requirements.*

In no way abrogates …

(m) *Subcontracts*.

Incident Response: capabilities considerations

- Creating an incident response policy and plan
- Developing procedures for performing incident handling and reporting
- Setting guidelines for communicating with outside parties regarding incidents
- Selecting a team structure and staffing model
- Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies)
- Determining what services the incident response team should provide
- Staffing and training the incident response team

NIST SP 800-61 r2; Computer Security Incident Handling Guide, page 1

Compile Lessons Learned

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident?
- Were the documented procedures followed?
- Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

NIST SP 800-61 r2; Computer Security Incident Handling Guide, pgs 38-39

Identify relevant metrics

- Number of incidents handled
- Time per incident
- Objective assessment of each incident
- Subject assessment of each incident (staff observations/comments)
- Incident response policies, plans, and procedures
- Tools and resources
- Team model and structure
- Incident handler training and education
- Incident documentation and reports
- The measures of success discussed earlier in this section.

NIST SP 800-61 r2; Computer Security Incident Handling Guide, pg 41

Periodically review program

- Incident response policies, plans, and procedures
- Tools and resources
- Team model and structure
- Contracts – scope, T&C's
- 3rd Party performance
- Incident handler training and education
- Incident documentation and reports
- The measures of success discussed earlier in this section.

NIST SP 800-61 r2; Computer Security Incident Handling Guide, pg 41

Develop – Use a checklist

	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

NIST SP 800-61 r2; Computer Security Incident Handling Guide, Table 3-5 pg 42

NIST Publications - partial

Resource Name	URL
NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*	http://csrc.nist.gov/publications/PubsSPs.html#800-53
NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*	http://csrc.nist.gov/publications/PubsSPs.html#800-83
NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*	http://csrc.nist.gov/publications/PubsSPs.html#800-84
NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*	http://csrc.nist.gov/publications/PubsSPs.html#800-86
NIST SP 800-92, *Guide to Computer Security Log Management*	http://csrc.nist.gov/publications/PubsSPs.html#800-92
NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*	http://csrc.nist.gov/publications/PubsSPs.html#800-94
NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*	http://csrc.nist.gov/publications/PubsSPs.html#800-115
NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*	http://csrc.nist.gov/publications/PubsSPs.html#800-128

NIST SP 800-61 r2; Computer Security Incident Handling Guide, Appendix E, page 63

Incident Response Organizations

Organization	URL
Anti-Phishing Working Group (APWG)	http://www.antiphishing.org/
Computer Crime and Intellectual Property Section (CCIPS), U.S. Department of Justice	http://www.cybercrime.gov/
CERT® Coordination Center, Carnegie Mellon University (CERT®/CC)	http://www.cert.org/
European Network and Information Security Agency (ENISA)	http://www.enisa.europa.eu/activities/cert
Forum of Incident Response and Security Teams (FIRST)	http://www.first.org/
Government Forum of Incident Response and Security Teams (GFIRST)	http://www.us-cert.gov/federal/gfirst.html
High Technology Crime Investigation Association (HTCIA)	http://www.htcia.org/
InfraGard	http://www.infragard.net/
Internet Storm Center (ISC)	http://isc.sans.edu/
National Council of ISACs	http://www.isaccouncil.org/
United States Computer Emergency Response Team (US-CERT)	http://www.us-cert.gov/

NIST SP 800-61 r2; Computer Security Incident Handling Guide, Appendix E, page 63

CYBER FRIDAY LIVE WEBINAR SERIES

- November 18, 2022

  Incident Identification, Reporting Requirements, and Recovery

  CLICK HERE for additional information

  Presented by Marc Violante, Wisconsin Procurement Institute

- December 2, 2022

  Designing and Using Security Exercises to Test and Improve Security Programs

  CLICK HERE for additional information

  Presented by Marc Violante, Wisconsin Procurement Institute

PRESENTED BY

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

TECHNOLOGY INNOVATION CENTER at RESEARCH PARK

NCMA NATIONAL CONTRACT MANAGEMENT ASSOCIATION WISCONSIN

ACQUISITION HOUR LIVE WEBINAR SERIES

- ~~November 16~~
  ~~**Certifications for Veteran Owned Businesses**~~
  –
- ~~November 16~~
  ~~**Preparing for One-on-One Buyer Meetings**~~
- November 29
  The HUBZone Program – Certification Benefits and Regulations
- January 10
  The SBA 8(a) Program and Small Disadvantaged Business (SDB) Program

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

…More information and registrations at wispro.org/events

Save the date

MARKETPLACE WISCONSIN

Plus 1-1 Buyer Meetings

The Contracting Academy

Developing and Growing Government Contractors

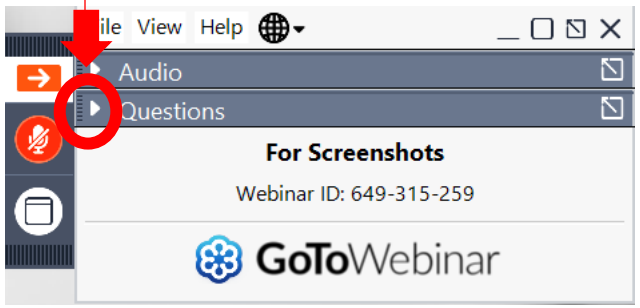
December 6-7, 2022

MarketplaceWisconsin.com

QUESTIONS?

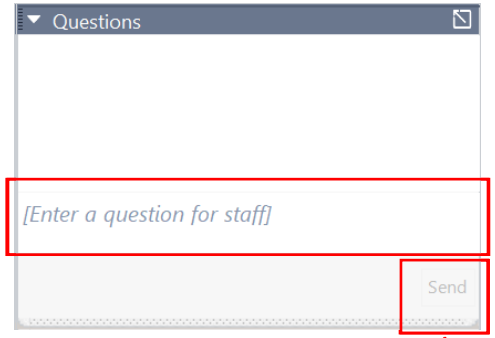
OPENING THE QUESTIONS BOX

Click here to access
within the Control Panel



USING THE QUESTIONS BOX

Type questions
here at any time
during a
presentation



Click Send when ready to submit a question

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
Cyber Friday

SURVEY

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

Cyber Friday

CONTINUING PROFESSIONAL EDUCATION

This webinar is eligible for 1 CPE credit.
For a certificate of this credit, please contact:

Caroline Boettcher
carolineb@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)
www.wispro.org

Marc Violante
Wisconsin Procurement Institute (WPI)
marcv@wispro.org | 920-456-9990

10437 Innovation Drive, Suite 320
Milwaukee, WI 53226