Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

Cyber Friday

The Cybersecurity Plan Looks Great

May 28, 2021




ABOUT WPI
SUPPORTING THE MISSION

Celebrating 34 Years of serving Wisconsin Business!

WPI 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**

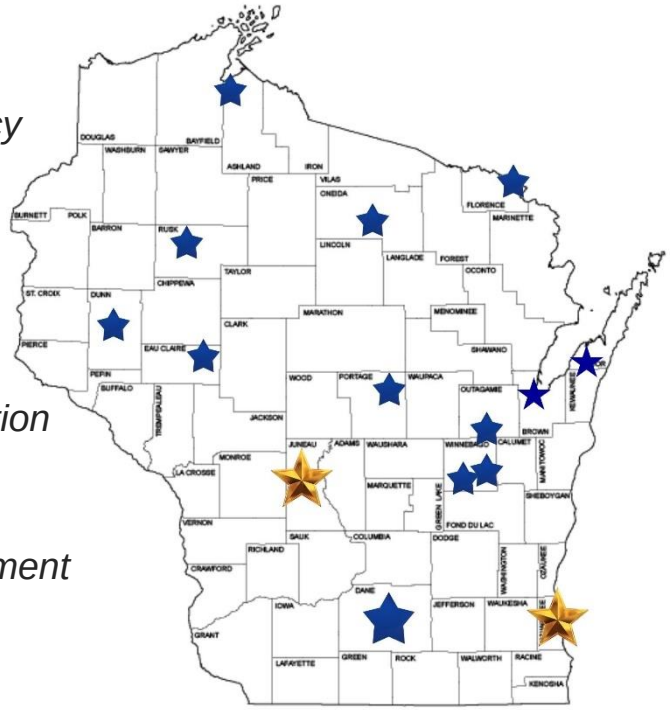
Last year WPI provided training at over 100 events and provided service to over 1,200 companies

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

WPI is a Procurement Technical Assistance Center (PTAC) funded in part by the Defense Logistics Agency (DLA), WEDC and other funding sources.

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)*
- **STEVENS POINT**
  - *IDEA Center*
- **APPLETON**
  - *Fox Valley Technical College*
- **SUPERIOR**
  - *Small Business Dev Center; UW Superior*
- **OSHKOSH**
  - *Fox Valley Technical College*
  - *Greater Oshkosh Economic Development Corporation*
- **EAU CLAIRE**
  - *Western Dairyland*
- **MENOMONIE**
  - *Dunn County Economic Development Corporation*
- **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*



5/28/21

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

Cyber Friday

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

The Cybersecurity Plan Looks Great

Marc N. Violante

May 28, 2021

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

Webinar Description

- If the internet “goes down,” your computer crashes, or if your database is corrupted, can your business survive? What if all your records are totally and irreparably damaged? That is what could happen with an errant click of a link or update that was not installed. Poof – all history – old and recent is extinguished. Companies seek to manage risk by outsourcing technical matters. This webinar will discuss this issue from the perspective of compliance with DoD requirements.

Be prepared

- **The U.S. government is working to draw attention to supply chain vulnerabilities, an issue that received particular attention late last year after suspected Russian hackers gained access to federal agencies and private corporations by sneaking malicious code into widely used software.**

- The National Counterintelligence and Security Center warned Thursday that foreign hackers are increasingly targeting vendors and suppliers that work with the government to compromise their products in an effort to steal intellectual property and carry out espionage. The NCSC said it is working with other agencies, including the Cybersecurity and Infrastructure Security Agency, to raise awareness of the supply chain issue.

Question more, trust less

- The malicious script was present for nearly two months between December 2020 and February 2021, and it collected information about the operating system, CPU, browser, input methods, camera, accelerometer, microphone, touchpoints, video card, time zone, geolocation, the screen, and browser plugins. In addition, it directed victims to a couple of sites that collected browser cipher fingerprints, which are used by some network defense solutions to detect connections from hosts infected with malware.
- Dragos determined that more than 1,000 computers accessed the watering hole during the two-month timeframe, including state and local government organizations, municipal water utility customers, and private firms related to the water industry.

https://www.securityweek.com/probe-florida-water-plant-hack-led-discovery-watering-hole-attack

Focus on the spirit & intent – not the words!

- It's not just Fortune 500 companies and nation states at risk of having IP stolen–even the local laundry service is a target.
- In one example, an organization of 35 employees was the victim of a cyber attack by a competitor.
- The competitor hid in their network for two years stealing customer and pricing information, giving them a significant advantage.

Hid for two years!

Internet Security Threat Report, Volume 21, April 2016, Symantec

So tempting; but should I?

Good morning,

I am sharing with you a Request for Proposal for BeneCom Technologie's innovative project. Please provide an offer and your availability for the scope of work. Should you have any questions, please do not hesitate to ask me.

RFP: #BCT-541Q0RFP-09

Please send a reply email to acknowledge receipt of this RFP.

Thank You,

Ann Walton
Sales Consultant
BeneCom *Technologies*

BENECOM Technologies
Cabling , Networks Phones , Security

Main: (225) 975-1043
Cell: (225) 892-2476
Fax: (504) 254-0008
Toll Free: (877) 966-7878

Understand what is at risk

A global insurance carrier refuses to write new ransomware policies in France, while insurers rewrite policies. Are we heading toward a day when ransomware incidents become uninsurable?

https://www.darkreading.com/risk/cyber-insurance-firms-start-tapping-out-as-ransomware-continues-to-rise/d/d-id/1341109

Handling Cyber Incidents

- (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: SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEC 2019);)

Use the correct definitions

- “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.

Know your contracts!

- **PGI 204.7303-4 DoD damage assessment activities.**
- (a) Prior to initiating damage assessment activities, the contracting officer shall verify that any contract identified in the cyber incident report includes the clause at DFARS 252.204-7012. If the contracting officer determines that a contract identified in the report does not contain the clause, the contracting officer shall notify the requiring activity that damage assessment activities, if required, may be determined to constitute a change to the contract.

Importance of the SSP & implementation

- (ii) Request a description of the contractor's implementation of the security requirements in NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (see http://dx.doi.org/10.6028/NIST.SP.800-171) in order to support evaluation of whether any of the controls were inadequate, or if any of the controls were not implemented at the time of the incident; and
- (iii) Provide a copy of the assessment of contractor compliance to the requiring activity, the DoD CIO at osd.dibcsia@mail.mil, and the other contracting officers listed in the cyber incident report.

https://www.acquisition.gov/dfarspgi/pgi-204.7303-3-cyber-incident-and-compromise-reporting

Know what requirements apply

- “Covered defense information” means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—
- (1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or
- (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

Develop Business Impact Analysis

The BIA is composed of the following three steps:

1. **Determine mission/business processes and recovery criticality.** Mission/business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum that an organization can tolerate while still maintaining the mission.
2. **Identify resource requirements.** Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.
3. **Identify recovery priorities for system resources.** Based upon the results from the previous activities, system resources can more clearly be linked to critical mission/business processes. Priority levels can be established for sequencing recovery activities and resources.

https://csrc.nist.gov/CSRC/media/Publications/sp/800-34/rev-1/final/documents/sp800-34-rev1_bia_template.docx

Define / Identify “essential”

- While all assets are valuable, they do not all have the same potential impact to the organization if they become unavailable or experience reduced capability. The organization should document and maintain the categorizations of its people, process, and technology assets based upon their relative importance. The prioritization of assets is critical, given that many agencies and organizations do not have sufficient resources to protect all assets to the same level of rigor and must prioritize the assets which must be recovered to support the mission.

NIST SP800-184 GUIDE FOR CYBERSECURITY EVENT RECOVERY; page 5

Identify interdependencies & prioritize

- Understanding recovery objectives relies upon understanding the interdependencies among resources. For example, it is frequently necessary to recover an identity or authentication server before recovering files, messaging services, and data stored and processed on servers across the infrastructure. There may also be less obvious dependencies, such as a person taking the result of a computation from system A and mailing it to someone else, who then manually enters it into system B. These dependencies need to be considered when setting objectives for recovery time and establishing the sequence for recovering systems.

NIST SP800-184 GUIDE FOR CYBERSECURITY EVENT RECOVERY; page 5

Containment, Eradication, and Recovery

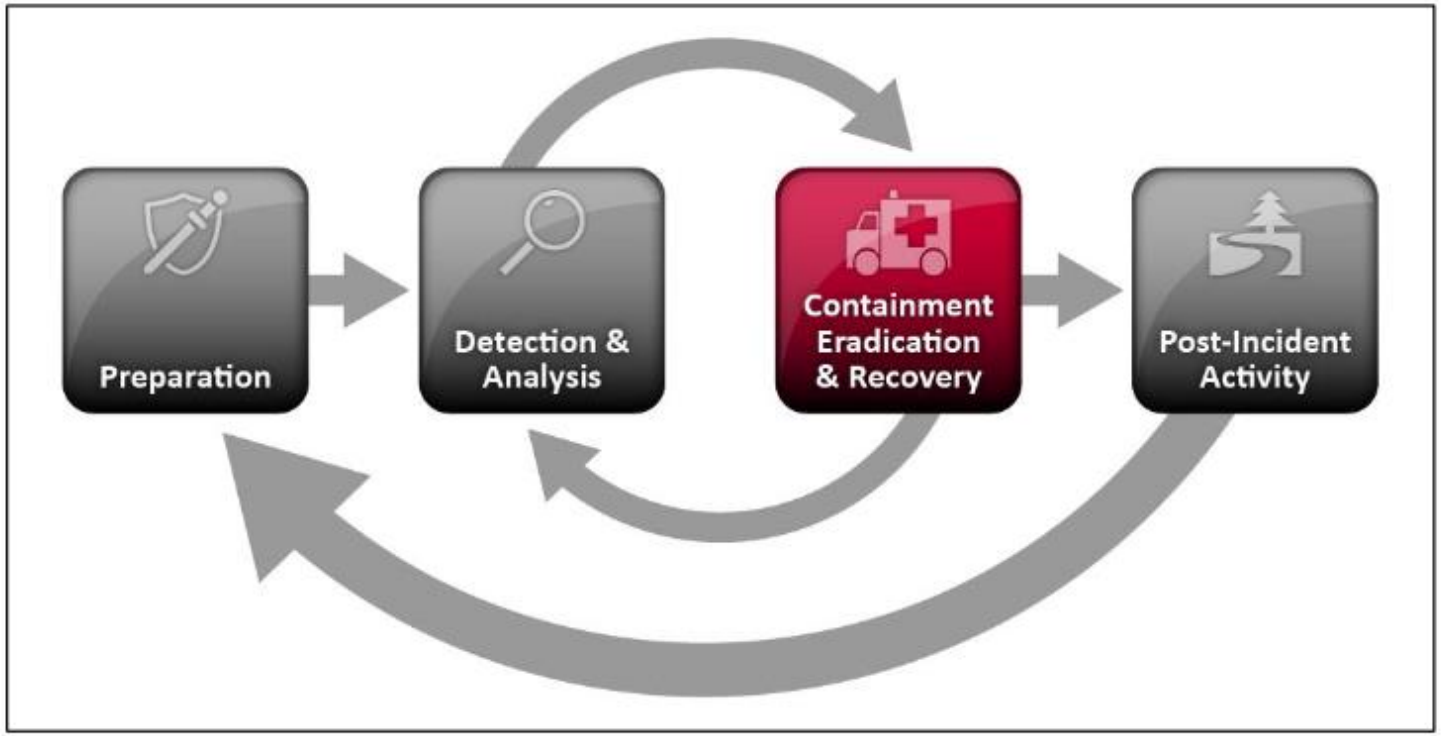


Figure 3-3. Incident Response Life Cycle (Containment, Eradication, and Recovery)

NIST 800-61 COMPUTER SECURITY INCIDENT HANDLING GUIDE; page 31

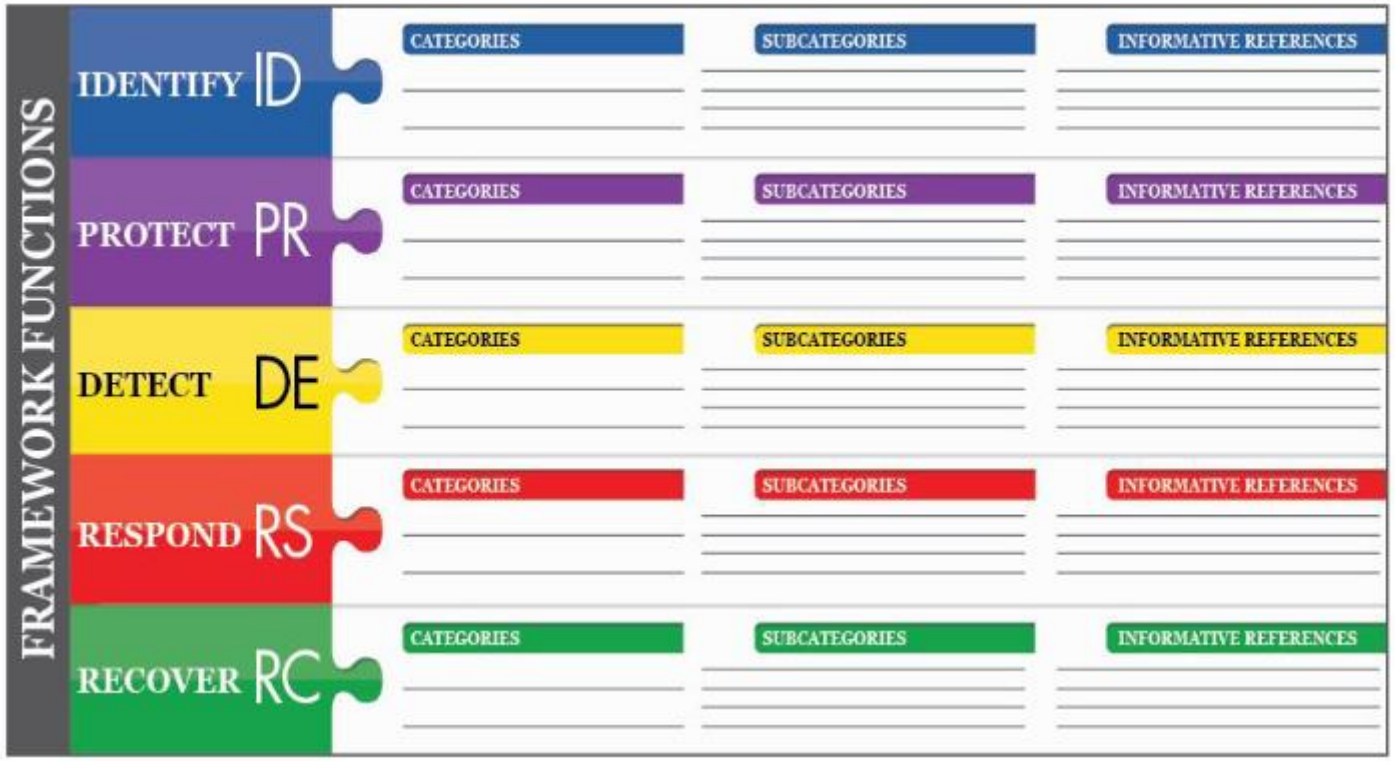
Visibility into systems is essential

Last year, a majority of incidents were related to improper usage, which includes installing unapproved software or accessing inappropriate materials. These types of incidents increased from 249 in 2017 to 1,103 in 2020. On the other hand, NASA also believes that the higher number of detected incidents is also a result of improved network visibility.

Attack Type	FY17	FY18	FY19	FY20
Attrition *(brute force network attack)*	9	10	0	2
Email	149	97	510	110
External/Removable Media	6	0	6	30
Impersonation *(appearing to be from a trusted source)*	0	1	0	4
Improper Usage	249	267	805	1,103
Loss/Theft of Equipment	430	392	346	274
Web	391	287	95	219
Other	50	83	126	43
TOTAL	**1,284**	**1,137**	**1,888**	**1,785**

https://www.securityweek.com/nasa-identified-over-6000-cyber-incidents-past-4-years

NIST Cybersecurity Framework



NIST Cybersecurity Framework, April 16, 2018, V 1.1 – figure 1, page 6

NIST Cybersecurity Framework

- Identify–Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities
- Protect–Develop and implement appropriate safeguards to ensure delivery of critical services.
- Detect–Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- Respond–Develop and implement appropriate activities to take action regarding a detected cybersecurity incident
- Recover–Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due toa cybersecurity incident.

NIST Cybersecurity Framework, April 16, 2018, V 1.1 – figure 1, pages 7-8

Cyber Event Recovery

NIST SP800-184 GUIDE FOR CYBERSECURITY EVENT RECOVERY; page iv

Information System Contingency Planning Process

CONTINGENCY PLANNING GUIDE FOR FEDERAL INFORMATION SYSTEMS – NIST 800-34

Types of Plans

CONTINGENCY PLANNING GUIDE FOR FEDERAL INFORMATION SYSTEMS – NIST 800-34

Cyber Incident Response Plan -def

a set of "procedures to enable security personnel to identify, mitigate, and recover from cyber attacks against an organization's information system(s)." The recovery plan is part of a cyber incident response plan with a concentration on the recovery element.

NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems

Incident Response Actions

- The current status of the incident(new, in progress, forwarded for investigation, resolved, etc.)
- A summary of the incident
- Indicators related to the incident
- Other incidents related to this incident
- Actions taken by all incident handlers on this incident
- Chain of custody, if applicable
- Impact assessments related to the incident
- Contact information for other involved parties (e.g., system owners, system administrators)
- A list of evidence gathered during the incident investigation
- Comments from incident handlers
- Next steps to be taken (e.g., rebuild the host, upgrade an application).[41]

COMPUTER SECURITY INCIDENT HANDLING GUIDE; NIST 800-61,page 31

Recovery – ground up / other

- Identify the scene – impacted device/system
- Secure “the scene”
- Awareness of legal requirements
- Forensic Image – secure
- Investigation
- Report – DoD / Other
- Determine span – what was effected
- List of software and licenses, contact information
- Assemble the team
- Who is in charge
- Determine cause
- Threat removal – sanitize system
- Review logs
- Verification
- Establish process to follow
- Initiate recovery

Key questions

- Is there a recovery plan?
- Where is it?
- Who are the team members?
- Who has access to it?
- Is it current?
- Has it been tested?
- Has it been updated?

Questions -2

- What are the facts as they are known?
- Is this a reportable incident?
- Is there a back-up?
- Is it current?
- Is it “the back-up” isolated from the network?
- Has it been tested? When?
- Is there a process/procedure in place by which the back up can be connected to a device without infecting the back-up?
- Has it “the process/procedure” been tested?

Cyber-Resilience

In a panel on building cyber-resilience, which was also this year's conference theme, panelists echoed many of Grobman's assertions. In "Building Cyber Resilience: Considerations for CISOs," Biju Hameed, director of technology infrastructure and operations at Dubai Airports, said his resilience planning is based on numbers and scientific assessment.

> "It's very important to define quantitative metrics in order to define resilience targets and capabilities," Hameed said. "Often there are a lot of perceptions and assumptions of what we need to do."

Abeer Khedr, information security director at the National Bank of Egypt, said the quest to determine which risks are most relevant is a constantly evolving process. With so much happening in digital banking and finance services, "There are no borders anymore, and the attack surface is constantly widening," Khedr says,

https://www.darkreading.com/edge/theedge/dont-let-scary-headlines-shape-your-companys-cyber-resilience-strategy/b/d-id/1341085

Are you resilient?

- Recovering normal operations for these services after a cyber event is often not a binary activity.
- Organizations must understand how to be resilient, planning how to operate in a diminished capacity or restore services over time based on services' relative priorities.
- DHS Risk Lexicon defines resilience as the -
  - "ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions." [DHS Risk Lexicon]

Assume the adversary will compromise or breach the system or organization.

- A fundamental assumption in any discussion of cyber resiliency is that a sophisticated adversary cannot always be kept out of a system or be quickly detected and removed from that system, despite the quality of the system design, the functional effectiveness of the security components, and the trustworthiness of the selected components. This assumption acknowledges that modern systems are large and complex entities and as such, adversaries will always be able to find and exploit weaknesses and flaws in the systems (e.g., unpatched vulnerabilities, misconfigurations), environments of operation (e.g., social engineering, user vulnerability), and supply chains.

NIST SP 800-160, VOLUME 2 ;DEVELOPING CYBER RESILIENT SYSTEMS A SYSTEMS SECURITY ENGINEERING APPROACH; page 73

Cyber resiliency goals

- Cyber resiliency, similar to security, is a concern at multiple levels in an organization. The cyber resiliency goals (i.e., anticipate, withstand, recover, and adapt) support the linkage between risk management decisions at the mission/business process and system levels and the organization's risk management strategy [SP 800-39].

INCIDENT RESPONSE

- Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. Requirement – 3.6.1
- Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. Requirement – 3.6.2
- Test the organizational incident response capability. Requirement – 3.6.3

SP 800-171, REVISION 2, PROTECTING CONTROLLED UNCLASSIFIED INFORMATION; page 27

Call List

- Company ownership
- System Owner
- Attorney
- PR firm – reputation
- Cyber Insurance
- Customers
- State/Local per laws and regulations
- Third party
- IT provider

Others as required

Incident Documentation

- Documenting system events, conversations, and observed changes in files can lead to a more efficient, more systematic, and less error-prone handling of the problem.
- Every step taken from the time the incident was detected to its final resolution should be documented and timestamped.
- Every document regarding the incident should be dated and signed by the incident handler.
- Information of this nature can also be used as evidence in a court of law if legal prosecution is pursued.
- Whenever possible, handlers should work in teams of at least two: one person can record and log events while the other person performs the technical tasks.

NIST 800-61 COMPUTER SECURITY INCIDENT HANDLING GUIDE; page 31

Develop/Use Incident Handling Checklist

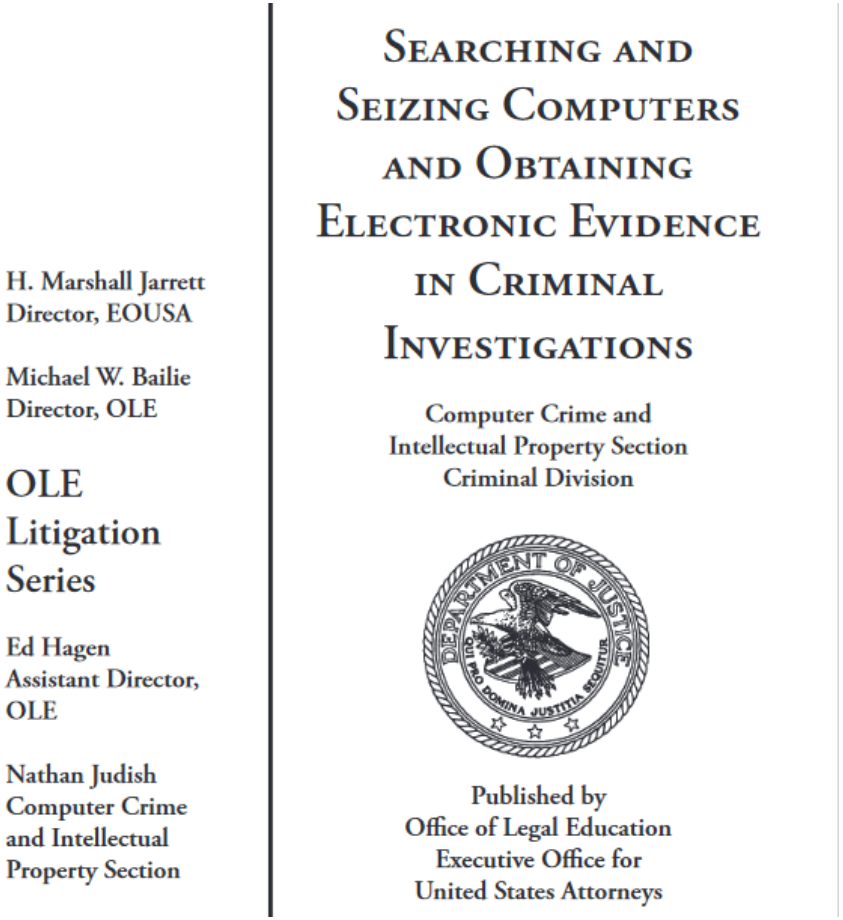
	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting 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)	

COMPUTER SECURITY INCIDENT HANDLING GUIDE; NIST 800-61,page 42

Be aware of specific requirements

- (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.

Assemble, Specify appropriate Resources



H. Marshall Jarrett
Director, EOUSA

Michael W. Bailie
Director, OLE

OLE
Litigation
Series

Ed Hagen
Assistant Director,
OLE

Nathan Judish
Computer Crime
and Intellectual
Property Section

SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS

Computer Crime and
Intellectual Property Section
Criminal Division

Published by
Office of Legal Education
Executive Office for
United States Attorneys

Note: 299 pages

https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

Internal *v.* External

- Considerations
  - Costs – savings v. talent v. premium v. use –
  - Usage – minor (routine) v. major
  - Information, awareness, data
  - Knowledge - capabilities
  - Resources – software, familiarity,
  - System knowledge, reliance on incomplete, inaccurate information
  - Maintenance
  - Ownership – “not mine/ours”; let them handle it
  - Availability

External

- Defined
- Contingency contract
- Response time-frame
- Level of effort
- Familiarity with topology, systems, software, security in-place
- Meetings with 3rd party IT service providers
- Vetting, by individuals for access
- System access – Carte Blanche, Managed, Direct - Indirect
- Federal information concerns – ITAR, JCP, CUI, NOFORN, Other
- On-site v. off-site v. blended

Identify Options

Start with the end in mind

Under the new rule, pipeline operators have 12 hours to report cyber incidents to DHS' Cybersecurity and Infrastructure Security Agency, which is partnering with TSA on pipeline security. These reports must describe the incident's projected impact, technical details associated with the intrusion and all current and planned responses. Within 30 days, companies must also assess how their cybersecurity practices line up with existing TSA guidance and develop plans to fix any gaps.

https://www.politico.com/news/2021/05/27/tsa-pipeline-breach-regulation-colonial-491123

Preparing through awareness

ACTIONS REQUIRED

A. Owner/Operators must designate and use a primary and at least one alternate Cybersecurity Coordinator at the corporate level.

1. Owner/Operators must provide in writing to TSA the names, titles, phone number(s), and email address(es) of the Cybersecurity Coordinator and alternate Cybersecurity Coordinator(s) within seven days of the effective date of this Security Directive, commencement of new operations, or change in any of the information required by this section.

2. The Cybersecurity Coordinator shall—

   a. Be a U.S. citizen who is eligible for a security clearance;

   b. Serve as the primary contact for cyber-related intelligence information and cybersecurity-related activities and communications with TSA and CISA;

   c. Be accessible to TSA and CISA 24 hours a day, seven days a week;

   d. Coordinate cyber and related security practices and procedures internally; and

   e. Work with appropriate law enforcement and emergency response agencies.

TSA Enhancing Pipeline Cybersecurity Security Directive Pipeline-2021-01, effective: May 28, 2021 12:01 am EST

Be aware of the larger picture

c. DoD contracts must require contractors to monitor CUI for aggregation and compilation based on the potential to generate classified information pursuant to security classification guidance addressing the accumulation of unclassified data or information. DoD contracts shall require contractors to report the potential classification of aggregated or compiled CUI to a DoD representative.

DoDI 5200.48, March 6, 2020; page 32

Identify & Integrate all reporting requirements

- (l) *Other safeguarding or reporting requirements.* The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

Determine Reporting Requirements

- (ii) Provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.

Attention to details

- (d) *Malicious software.* When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

Be prepared – flow down (alert) as needed

- (3) *Medium assurance certificate requirement.* In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see https://public.cyber.mil/eca/
  - Time
  - Cost
  - Information
  - usage

Don’t be caught off-guard

- (D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/resources/documents/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

DFARS 252.204-7012: SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEC 2019); para (d)

Don’t be caught off-guard -2

- (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.
- This statement applies to cloud computing data centers operated as an extension of a contractor’s internal IT system. DoD normally will not require physical access if the cloud services provider captures, preserves, and protects images and the state of all systems known to be affected by a cyber incident as separately required by paragraph (e) of DFARS clause 252.204-7012. However, in highly unusual circumstances, there may still be some cases when DoD may require physical access to equipment. Because the need for access is driven by the circumstances surrounding the cyber incident, DoD is not able to waive this requirement

DFARS 252.204-7012: SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEC 2019); para (f)
http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html

Identify immediate actions

- (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.

UPCOMING TRAINING - EVENTS

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

NDIA Great Lakes Great Rivers Iowa-Illinois

NDIA MIDWEST REGIONAL CONFERENCE SERIES

JUNE 2

2:00 – 3:00 PM

The National Defense Industrial Association's (NDIA) Great Lakes, Great Rivers and Iowa-Illinois chapters, partnered with the Wisconsin Procurement Institute (WPI), invite you to attend the first of a three-part virtual series featuring leaders in U.S. Defense. In this series, you will have the opportunity to learn about current issues, programs, and priorities critical to Defense contractors and subcontractors.

Registration Now Open

…More at wispro.org/events

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

5/28/21

WBDC IGNITES BUSINESS GROWTH

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

Partnering With Purpose Series

Session 1

FUNDAMENTALS OF TEAMING AND PARTNERING

June 15 | 10 am – Noon REGISTER HERE

Session 2

CHALLENGES IN DEVELOPING SUCCESSFUL BUSINESS TEAMS AND PARTNERSHIPS

July 20 | 10 am – Noon REGISTER HERE

Session 3

A ROADMAP TO DEVELOPING SUCCESSFUL TEAMS AND PARTNERSHIPS

Aug 17 | 10 am – Noon REGISTER HERE

Registration Now Open

…More at wispro.org/events

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

CYBER FRIDAY LIVE WEBINAR SERIES

May 28, 2021 The Cybersecurity Plan Looks Great

June 11, 2021 Blockchain

June 25, 2021 The Role of Standardization in Cybersecurity Plans

Register at: https://www.wispro.org/faqs/what-is-wpis-current-cyber-friday-webinar-schedule/

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

- June 16, 2021

  Acquisition Hour: The New SAM.gov
  CLICK HERE for additional information
  Presented by Kim Garber, Wisconsin Procurement Institute

- July 13, 2021

  Acquisition Hour: The Spend to the End
  CLICK HERE for additional information
  Presented by Benjamin Blanc, Wisconsin Procurement Institute

- July 21, 2021

  Acquisition Hour: Government Property Management for Federal Contractors and Subcontractors
  CLICK HERE for additional information
  Presented by Benjamin Blanc, Wisconsin Procurement Institute

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

…More at wispro.org/events

CYBERSECURITY – UPDATE – DECEMBER 2020

- CMMC -
  - Implementation continues
  - Pathfinder contracts to be announced soon – article, Dec 1, 2020
    - CMMC requirements will be included
  - Full implementation expected by Oct 2025
- New clauses and requirements –
  - DFARS 252.204-7019
  - DFARS 252.204-7020 – applies to contracts subject to 252.204-7012
    - With few exceptions, these requirements apply to all Primes and Subcontractors
    - Consistent with philosophy shift of self-attest to verifiable
    - Three levels – Base – self-performed , Medium & High - DCMA

252.204-7020 – BASIC ASSESSMENT

- Requires
  - System Security Plan(SSP)
  - Plan of Action – with dates for outstanding items
  - Basic Assessment
- Six elements uploaded to Supplier Performance Risk System (SPRS)
  1. System Security Plan name (if more than one system is involved)
  2. Brief description of Plan Architecture
  3. CAGE code associated with SSP
  4. Date Assessment performed
  5. Summary Score
  6. Date a score of 110 to be achieved

CURRENT CYBER REQUIREMENTS

- FAR 52.204-21 – Federal Contract Information
- DFARS 252.204-7012
- Requirements cited in solicitation/contract

Need assistance – please contact Marc Violante from WPI at marcv@wispro.org or 920-456-9990

CONTINUING PROFESSIONAL EDUCATION

CPE Certificate available, please contact:

Benjamin Blanc

benjaminb@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