Wisconsin Procurement Institute

ACQUISITION HOUR WEBINAR

IT management requirements for DOD Contractors and Subcontractors

Sponsored by:

NCMA NATIONAL CONTRACT MANAGEMENT ASSOCIATION

NDIA National Defense Industrial Association

May 20, 2015

Wisconsin Procurement Institute

Providing expert technical assistance to FEDERAL, STATE and LOCAL GOVERNMENT Contractors And Subcontractors

A Procurement Technical Assistance Center (PTAC)

Serving the Wisconsin Business Community

WPI Offices located at:

Milwaukee County Research Park
10437 Innovation Drive, Suite 320
Milwaukee, WI 53226
414-270-3600 FAX: 414-270-3610

Juneau County Economic Development Corp.
122 Main St - Camp Douglas, WI 54618
608-427-2455 FAX: 608-427-2086

Western Dairyland EOC, Inc.
418 Wisconsin St. - Eau Claire WI 54703
608-427-2455 FAX: 608-427-2086

Fox Valley Technical College – DJ Bordini Center
5 Systems Drive – Appleton WI 54912
920-840-3771 FAX: 414-270-3610

Racine County Economic Development Corporation – Launch Box
141 Main Street, Suite 2, Racine, WI 53403
414-270-3600 FAX: 414-270-3610

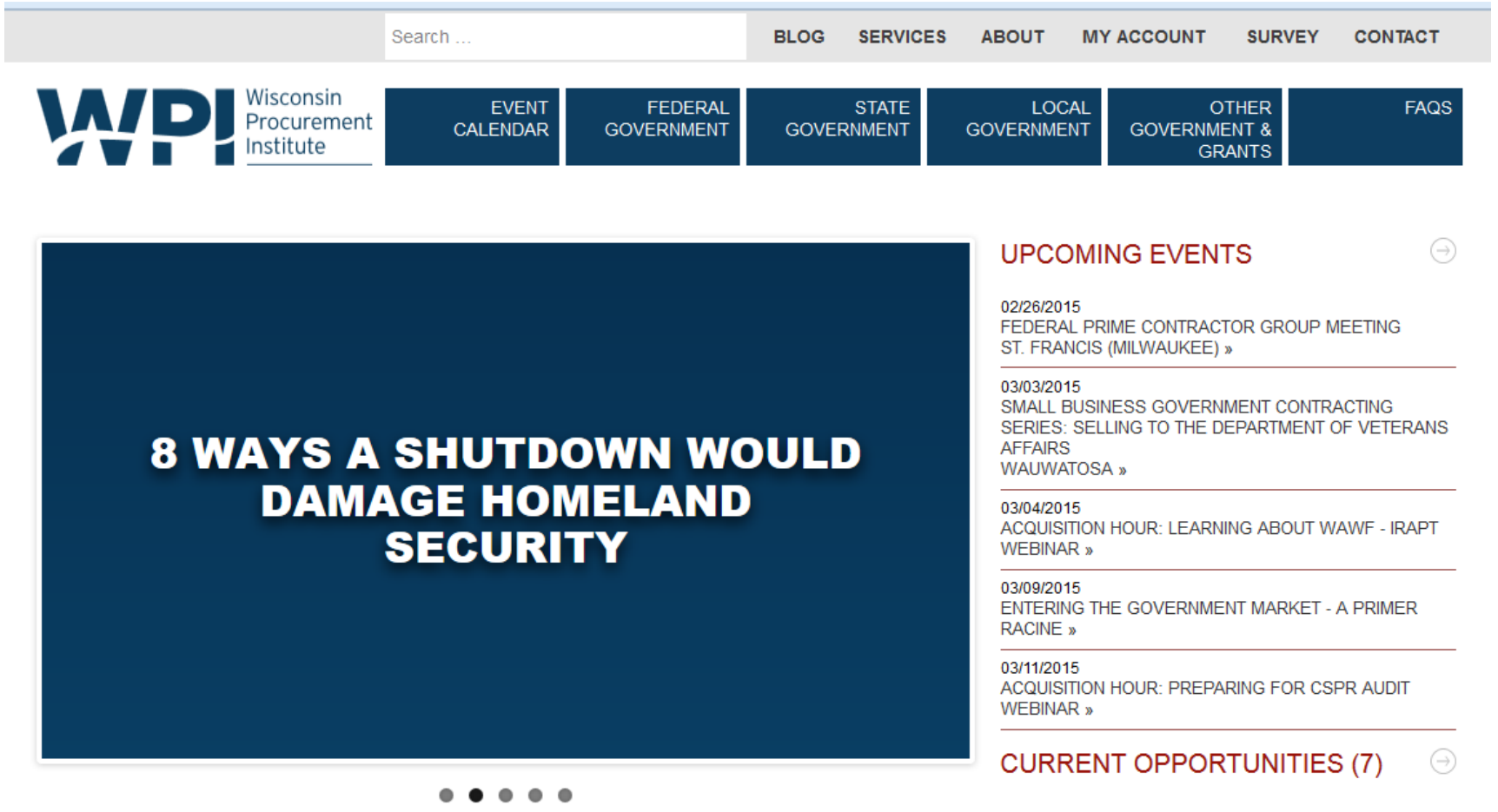
Madison Enterprise Center
100 S. Baldwin St., Madison, WI 53703
608-444-0047 FAX: 414-270-3610

Food Enterprise & Economic Development (FEED)
1219 N. Sherman Ave., Madison, WI 53704
608-444-0047 FAX: 414-270-3610

Wausau Region Chamber of Commerce
200 Washington Street, Wausau, WI 54403
920-456-9990 FAX: 414-270-3610

www.wispro.org - info@wispro.org

May 27, 2015


Search ...
BLOG
SERVICES
ABOUT
MY ACCOUNT
SURVEY
CONTACT
WPI
Wisconsin Procurement Institute
EVENT CALENDAR
FEDERAL GOVERNMENT
STATE GOVERNMENT
LOCAL GOVERNMENT
OTHER GOVERNMENT & GRANTS
FAQS
8 WAYS A SHUTDOWN WOULD DAMAGE HOMELAND SECURITY
UPCOMING EVENTS
02/26/2015
FEDERAL PRIME CONTRACTOR GROUP MEETING
ST. FRANCIS (MILWAUKEE) »
03/03/2015
SMALL BUSINESS GOVERNMENT CONTRACTING SERIES: SELLING TO THE DEPARTMENT OF VETERANS AFFAIRS
WAUWATOSA »
03/04/2015
ACQUISITION HOUR: LEARNING ABOUT WAWF - IRAPT WEBINAR »
03/09/2015
ENTERING THE GOVERNMENT MARKET - A PRIMER
RACINE »
03/11/2015
ACQUISITION HOUR: PREPARING FOR CSPR AUDIT WEBINAR »
CURRENT OPPORTUNITIES (7)
GET STARTED WITH THE BASICS
Questions & answers on how to get started.
GET STARTED
SIGN-UP FOR OUR NEWSLETTER
Stay up-to-date with the latest WPI news.
SIGN UP
HAVE A QUESTION? WE'RE HERE TO HELP.
One of our staff of experts is available to answer your questions.
GET HELP

Wisconsin Procurement Institute

EVENT CALENDAR | FEDERAL GOVERNMENT | STATE GOVERNMENT | LOCAL GOVERNMENT | OTHER GOVERNMENT & GRANTS | FAQS

GET STARTED WITH THE BASICS

Questions & answers on how to get started.

GET STARTED

SIGN-UP FOR OUR NEWSLETTER

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

SIGN UP

HAVE A QUESTION? WE'RE HERE TO HELP.

One of our staff of experts is available to answer your questions.

GET HELP

SERVICES OFFERED BY WPI

- FREE Bid Matching Services
- Individual Counseling and Assistance
- Locating Local, State and Federal Opportunities
- Government Market Strategy Development
- Training in use of Government websites and tools
- Assistance with System for Award Management (SAM) Registration
- Assisting in Market Research Process
- Development of Market Profile
- Small Business Subcontracting Plans-Development, Outreach and Reporting
- Small Group Training
- Outreach and training with Local, State and Federal agencies
- Assist with Pre and Post Award Functions
- Assistance with Agency Specific Contracting Requirements
- Assistance with Contracting Regulations and Requirements, including FAR, DFAR, CFR
- Assistance with GSA Schedule Preparation and Administration
- Assistance with Local, State and Federal Certifications, including:
  - Service Disabled & Veteran Owned Small Business, HUBZone, Woman Owned Small Business, 8(a) Business Development Program
  - State
  - Local
  - DBE
- Bid Review and Submission Assistance
- Proposal and Assistance, Review and Submission Assistance
- Capabilities Statement and Related Government Marketing Material Development
- Assistance in Locating and Developing Teaming Partners and Subcontractors
- Updated Government Market Information

Wisconsin Procurement Institute
10437 Innovation Dr., Suite 320
Milwaukee, WI 53226
Telephone 414-270-3600
FAX 414-270-3610
www.wispro.org
Executive Director – Aina Vilumsons
info@wispro.org

Safeguarding Information

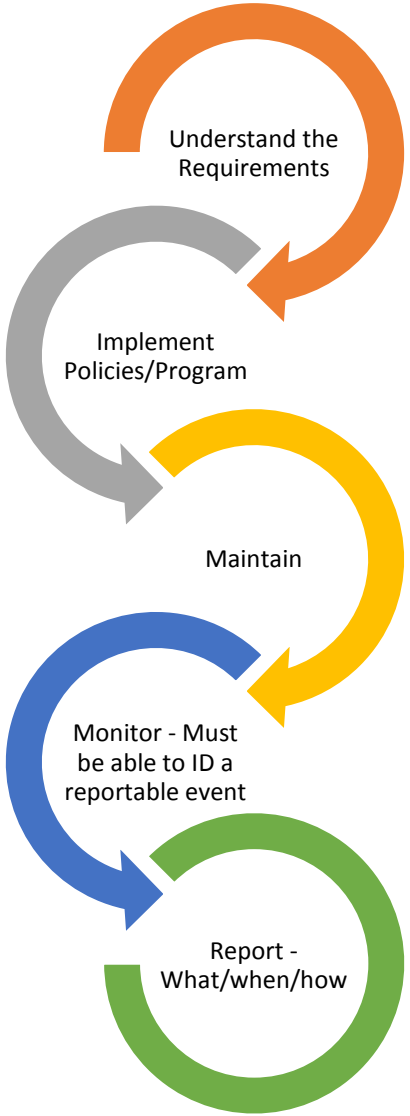
Marc N. Violante

WPI – Acquisition Hour

IT Management Requirements for DoD Contractors and Subcontractors

May 20, 2015

Wisconsin Procurement Institute



Wisconsin Procurement Institute

References (cited/discussed)

- DFARS – 252.204-7000 – Disclosure of Information
- SUBPART 204.73—SAFEGUARDING UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION
- DFARS – 252.204-7012 -- Safeguarding of Unclassified Controlled Technical Information
- DoD Instruction 5230.24 -- Distribution Statements on Technical Documents
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53

Critical point

- These clauses/requirements are included in many solicitations.
- Determining
  - If – when - or to what they apply is the contractor's responsibility
  - In some cases it may make sense to ask or request that either one or both clauses be removed from a solicitation
- If they do apply –
  - Developing a tracking systems, especially if there are several subcontractors
  - Recalculate due date and reasonableness given potential time delays
  - Time and cost for subcontractors training
  - Identification of new subcontractors

What data/information is on your computer?
On your Network?

Wisconsin Procurement Institute

General Classifications of Information

Public Domain

Unclassified Controlled Technical Information

For Official Use Only

Classified – Confidential, Secret, Top Secret – etc.

Who has access?

Who has access?

Who has access?

Who has access?

Who has access?

Who has access?

Who has access?

Who has access?

Who has access?

Who has access?

Who has access?

Who has access?

Wisconsin Procurement Institute

Hypotheticals

- Do you manage the contents (files) on USBs that you share?
  - With subcontractors
  - Vendors
  - At events – public use terminals
- Can you be sure that the contents of the drive were not copied?
- Do you pick up and use “Thumb Drives” from trade shows?
- Other sources?

Hypotheticals – 2

- Do you save all files to your laptop?
- Do you keep a record of information saved to your laptop?
- Do you travel with your laptop?
- How do you protect the data on your laptop?
  - Is it encrypted?
- What would happen is you lost or had your laptop stolen?

Office procedures

- Who has access to your network?
- Does each employee have their own computer?
- Are computers shared?
- Do all employees have access to all information?
- Are passwords used to protect folders and files?
- Are employees required to change their passwords?
- Does each computer have anti-virus software loaded and enabled?
- Are IT functions accomplished in-house or by a third party?
- Do you monitor your network?

Personnel

- Are employees provided any IT training?
- Are employees screened prior to granting access to the IT system?
- Are third party vendors who have access to the IT system screened?
- Do you travel with your business laptop?

Business Relationships

- Do you openly share information/files with suppliers?
- Do you verify that your suppliers can have access to information that you plan to share?
- Are you aware of the different regulations governing protection of data?
- Have you read and researched the regulations that apply to governing data and unclassified information?
- Do you pass down these requirements to your subcontractors/suppliers?

Mother may I? - 252.204-7000 Disclosure of Information

- (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

As prescribed in 204.404-70(a), use the following clause: DISCLOSURE OF INFORMATION (AUG 2013)

Wisconsin Procurement Institute

DFARS 204.7302 Policy

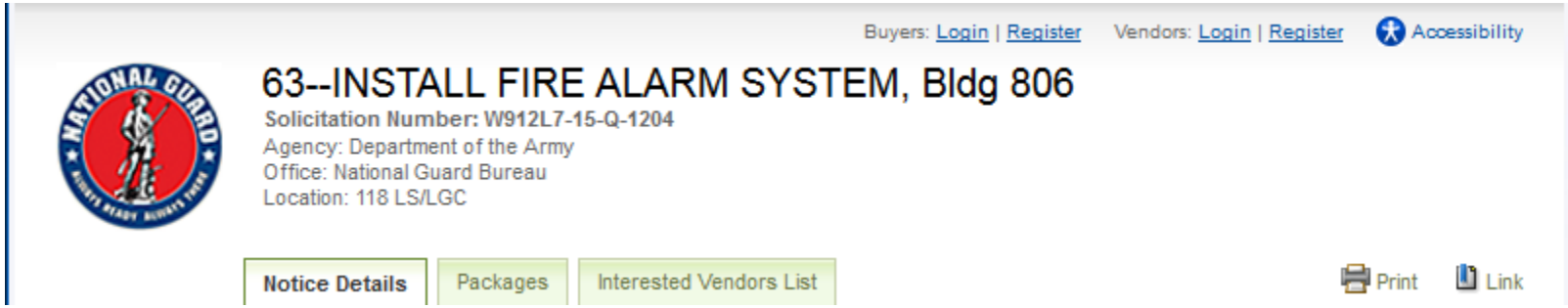
- DoD and its contractors and subcontractors will provide adequate security to safeguard unclassified controlled technical information on their unclassified information systems from unauthorized access and disclosure.

SUBPART 204.73—SAFEGUARDING UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION *(Revised December 16, 2014)*

Applicability

- 252.204-7012 Safeguarding of Unclassified Controlled Technical Information
    - Page 8 of the DLA Master Solicitation

Beware!



The following clauses are applicable to this acquisition … :

52.252-2 Clauses Incorporated by Reference
252.204-7000 Disclosure of Information
252.212-7001 Contract Terms and Conditions Required to Implement Statutes or Executive Orders Applicable to Defense Acquisitions of Commercial Items.
252.222-7006 quote mark Restrictions on the Use of Mandatory Arbitration Agreements

FBO Search returned 95 solicitations that include 252.204-7000 as a clause

Wisconsin Procurement Institute

Probably not the intended approach

Wisconsin Procurement Institute

Awareness is key – active efforts/processes

Wisconsin Procurement Institute

Controlled Technical Information

- Technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.
- - is to be marked with one of the distribution statements B-through-F, in accordance with DoD Instruction 5230.24, Distribution Statements on Technical documents.
- The term does not include information that is lawfully publicly available without restrictions.

Wisconsin Procurement Institute

Distribution Statement – selection criteria

1. Criteria specified in Enclosure 3 of Reference (l).
2. Export controls in accordance with Reference (d); parts 120-130 of title 22, Code of Federal Regulations (CFR) (also known and hereinafter referred to as the “International Traffic in Arms Regulations” (ITAR)) (Reference (q)); and parts 730-774 of title 15, CFR (also known and hereinafter referred to as the “Export Administration Regulations” (EAR)) (Reference (r)).
3. Intellectual property and data rights licenses for contract deliverables in subpart 227.71 of title 48, CFR (Reference (s)).
4. CPI protection in accordance with Reference (p) Critical Program Information

DoDI 5230.24, August 23, 2012, Enclosure 3 pages 10 & 11 – references Enclosure 1

Distribution Statements

- A. Approved for public release.
- B. U.S. Government agencies only
- C. U.S. Government agencies and their contractors
- D. Department of Defense and U.S. DoD contractors only
- E. DoD Components only
- F. Further dissemination only as directed by

DoD Instruction 5230.24 August 23, 2012

Compromise

- Means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional disclosure, modification, destruction, or loss of an object or the copying of information to unauthorized media may have occurred.

252.204-7012 Safeguarding of Unclassified Controlled Technical Information - Definitions

Media

- Means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which information is recorded, stored, or printed within an information system.

252.204-7012 Safeguarding of Unclassified Controlled Technical Information - Definitions

Cyber incident

- “Cyber incident” means actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.

252.204-7012 Safeguarding of Unclassified Controlled Technical Information. (c)

Safeguarding requirements and procedures (UCTI)

- The Contractor shall provide adequate security to safeguard unclassified controlled technical information from compromise.

- To provide adequate security, the Contractor shall-
  - Implement information systems security in its project, enterprise, or company-wide unclassified information technology system(s) that may have unclassified controlled technical information resident on or transiting though them.

252.204-7012 Safeguarding of Unclassified Controlled Technical Information – (b)

Information systems security program

- --- at a Minimum
- Implement (i) the specified National Institute of Standards and Technology (NIST) Special Publication(SP) 800-53 security controls identified in the following table (see – DFAR 252.204-7012)
- If a NIST control is not implemented, the Contractor shall submit to the Contracting Officer a written explanation of how –
  - The required security control identified in the table is not applicable
  - An alternative control or protective measure is used to achieve equivalent protection.
  - Other security measures, in addition to those identified to provide adequate security relative to the environment.

Other requirements

- This clause does not relieve the Contractor of the requirements specified by applicable statutes or other Federal and DoD safeguarding requirements for Controlled Unclassified Information (CUI) as established by Executive Order 13556, as well as regulations and guidance established pursuant thereto.

252.204-7012 Safeguarding of Unclassified Controlled Technical Information. (c)

Wisconsin Procurement Institute

DFARS – Reporting Requirements

- When safeguarding is applied to controlled technical information resident on or transiting contractor unclassified information systems—
- (1) Contractors must report to DoD certain cyber incidents that affect unclassified controlled technical information resident on or transiting contractor unclassified information systems.
- Detailed reporting criteria and requirements are set forth in the clause at 252.204-7012, Safeguarding of Unclassified Controlled Technical Information.

SUBPART 204.73—SAFEGUARDING UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION *(Revised December 16, 2014)*

Reporting requirement

- The Contractor shall report as much of the following information as can be obtained to the Department of Defense via (http://dibnet.dod.mil/) within 72 hours of discovery of any cyber incident, as described in paragraph (d)(2) of this clause, that affects unclassified controlled technical information resident on or transiting through the Contractor's unclassified information systems:

Reporting – information required

- (i) Data Universal Numbering System (DUNS).
- (ii) Contract numbers affected unless all contracts by the company are affected.
- (iii) Facility CAGE code if the location of the event is different than the prime Contractor location.
- (iv) Point of contact if different than the POC recorded in the System for Award Management (address, position, telephone, email).
- (v) Contracting Officer point of contact (address, position, telephone, email).
- (vi) Contract clearance level.
- (vii) Name of subcontractor and CAGE code if this was an incident on a Sub-contractor network.
- (viii) DoD programs, platforms or systems involved.
- (ix) Location(s) of compromise.
- (x) Date incident discovered.
- (xi) Type of compromise (e.g., unauthorized access, inadvertent release, other).
- (xii) Description of technical information compromised
- (xiii) Any additional information relevant to the information compromise.

252.204-7012 Safeguarding of Unclassified Controlled Technical Information (d) (1)

Security Plan – topical areas – 51 separate elements

- AC: Access Control
- AT: Awareness and Training
- AU: Audition and Accountability
- CM: Configuration Management
- CP: Contingency Planning
- IA: Identification and Authentication
- IR: Incident Response
- MA: Maintenance
- MP: Media Protection
- PE: Physical & Environmental Protection
- PM: Program Management
- RA: Risk Assessment
- SC: System & Communication Protection
- SI: System & Information Integrity

252.204-7012 Safeguarding of Unclassified Controlled Technical Information (Table - 1)

Security Plan – topical areas – 51 separate elements

TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

ID	FAMILY	ID	FAMILY
● AC	Access Control	● MP	Media Protection
● AT	Awareness and Training	● PE	Physical and Environmental Protection
● AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
● CM	Configuration Management	● RA	Risk Assessment
● CP	Contingency Planning	SA	System and Services Acquisition
● IA	Identification and Authentication	● SC	System and Communications Protection
● IR	Incident Response	● SI	System and Information Integrity
● MA	Maintenance	● PM	Program Management

252.204-7012 Safeguarding of Unclassified Controlled Technical Information (Table ●1) - Applicable

Table – 1 copied from NIST Special Publication 800-53 Revision 4, Chapter 2

WPI Wisconsin Procurement Institute

Risk Management Framework

- **Step 1:** *Categorize* the information system based on a FIPS Publication 199 impact assessment;28
- **Step 2:** *Select* the applicable security control baseline based on the results of the security categorization and apply tailoring guidance (including the potential use of overlays);
- **Step 3:** *Implement* the security controls and document the design, development, and implementation details for the controls;
- **Step 4:** *Assess* the security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;29
- **Step 5:** *Authorize* information system operation based on a determination of risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation and use of the information system and the decision that this risk is acceptable; and
- **Step 6:** *Monitor* the security controls in the information system and environment of operation on an ongoing basis to determine control effectiveness, changes to the system/environment, and compliance to legislation, Executive Orders, directives, policies, regulations, and standards.

Special Publication 800-53 Revision 4 - Security and Privacy Controls for Federal Information Systems and Organizations (Chapter 2, page 9)

Security Objectives

- Availability
  - “Ensuring timely and reliable access to and use of information…” [44 U.S.C., SEC. 3542]
  - A loss of *availability* is the disruption of access to or use of information or an information system.
- Integrity
  - “Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…” [44 U.S.C., Sec. 3542]
  - A loss of *integrity* is the unauthorized modification or destruction of information.
- Confidentiality
  - “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…” [44 U.S.C., Sec. 3542]
  - A loss of *confidentiality* is the unauthorized disclosure of information.

3.1 SELECTING SECURITY CONTROL BASELINES

- Security Categorization
  - Determine the criticality and sensitivity of the information to be ---
    - Processed
    - Stored
    - Transmitted
  - Reference FIPS 199.58
  - Purpose – determining potential adverse impact
  - Outcome – helps guide and inform on the selection of appropriate security controls
  - Controls are commensurate with the potential adverse impact on organizational operations and assets

Security Categorization

- determine the criticality and sensitivity of the information to be processed, stored, or transmitted by those systems
- Concept –
  - determining the potential adverse impact for organizational information systems
- The security controls selected for information systems are commensurate with the potential adverse impact on organizational operations and assets, individuals, other organizations, or the Nation if there is a loss of confidentiality, integrity, or availability

NIST SP 800-53r4 para 3.1

Security Categorization (generalized format)

- **SC** information system =
  - {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},
  - acceptable values for potential impact are:
    - low
    - moderate
    - high.

NIST SP 800-53r4 para 3.1

Low Impact

- The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. [4] A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

NIST SP 800-60V1 2.2 Impact Assessment (Contents from FIPS 199)

Moderate Impact

- The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

NIST SP 800-60V1 2.2 Impact Assessment (Contents from FIPS 199)

High Impact

- The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

NIST SP 800-60V1 2.2 Impact Assessment (Contents from FIPS 199)

Confidentiality, integrity or availability

- Categorize information systems as
  - Low-impact
  - Moderate-impact
  - High-impact
- Potential impact values assigned to the security objective are the highest values

Key areas of concern

The generalized format for expressing the security category (SC) of an information system is:

SC information system = {(confidentiality, impact), (integrity, impact), (availability, impact)}, where the acceptable values for potential impact are low, moderate, or high.

Since the potential impact values for confidentiality, integrity, and availability may not always be the same for a particular information system, the high water mark concept (introduced in FIPS Publication 199) is used in FIPS Publication 200 to determine the impact level of the information system for the express purpose of selecting the applicable security control baseline from one of the three baselines identified in Appendix D.60

- A low-impact system is defined as an information system in which all three of the security objectives are low.
- A moderate-impact system is an information system in which at least one of the security objectives is moderate
- A high-impact system is an information system in which at least one of the security objectives is high

Wisconsin Procurement Institute

questions?

Contact for more information

- Marc Violante: marcv@wispro.org

Upcoming WPI Events

- ***Small Business Government Contracting Series continues the first and third Tuesday of each month through June, 2015*** – *Milwaukee, WI*
- ***Acquisition Hour (Weekly Webinar) through June, 2015***
- ***Doing Business with the National Park Service*** – *June 23, 2015 – Ashland, WI*
- ***9th Annual Volk Field Small Business Conference*** – *July 29 – 30, 2015 – Camp Douglas, WI*
- ***Marketplace 2015*** – *October 29-30, 2015 – Milwaukee, WI*