Welcome to Safeguarding Unclassified Control Technical Information & Cybersecurity Contract Requirements

Moderator: Charysse Knotts, Black & Veatch

Speakers:

• Jonathan Hard, CEO & President, H2L Solutions Inc.
• Ken Metzler, CIO, NAVFAC EURAFSWA
OUTLINE

• Challenges with implementing DFARS and NIST 800-171 compliance
• What businesses need to know?
• Executive Order 13556
• What types of information systems that process or store DoD’s unclassified information?
• CUI Registry- Categories/Subcategories
• FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems
• DFARS 7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
• 252.204-7008 Compliance with Safeguarding Covered Defense Information Controls
• Additional updates
• Danger of not implementing FAR 52.204-21 and DFARS 252.204-7012
CHALLENGES OF IMPLEMENTING FAR 52.204-21 AND DFARS 252.204-7012 & NIST 800-171

- Vague requirements
- Not enough time
- Tight budget
- Meshing NIST 800-171 with your information security program
- NIST 800-171 is a shifting target
- Maintaining compliance
- Missing/missed the NIST 800-171 Deadline
  - Liabilities for not being in compliance by 31 Dec 2017
- Consequences of NIST 800-171 Non-Compliance
- New changes being proposed by DoD
WHAT BUSINESSES NEED TO KNOW?

• The threats facing Department of Defense’s (DoD) unclassified information have dramatically increased as we provide more services online, digitally store data and rely on contractors for a variety of information technology services.

• Recent high-profile incidents involving, personal, industry and government information demand that information system security requirements are clearly, effectively and consistently communicated to both government and industry.

• Businesses may not be able to do business with the government without having the proper security procedures in place in the future.

• Immediate Action: Implement the National Institute of Standards and Technology (NIST) 800-171 Security by December 31, 2017.
EXECUTIVE ORDER 13556

- Establish CUI Program

- Executive Agent (EA) to implement the E.O. and oversee department and agency actions to ensure compliance

- An open and uniform program to manage all unclassified information within the executive branch that requires safeguarding and dissemination controls as required by law, regulation, and Government-wide policy
WHAT TYPES OF INFORMATION SYSTEMS THAT PROCESS OR STORE DOD’S UNCLASSIFIED INFORMATION?

• Contractor’s Internal Information System: An information system that is owned, or operated by or for, a contractor.

• DoD Information System, to include:
  • DoD-owned and/or operated Information System: An information system owned or operated by the DoD or by another government organization on behalf of the DoD.
  • Contractor System operated on behalf of DoD: The term "on behalf of" as used here means when a contractor builds an information system for the DoD or operates an information system for the DoD, e.g., an email provider or payroll system, or provides processing services for DoD. e.g., cloud-service providers.
CUI REGISTRY - CATEGORIES/SUBCATEGORIES

Some categories of CUI may be handled by relatively few users. Other CUI includes many types of information within a category, and is routinely accessible by a wide range of users.

ALL CUI categories and subcategories in the Registry have been approved based on safeguarding and dissemination requirements in law, regulation and Government-wide policy.

<table>
<thead>
<tr>
<th>Categories</th>
<th>Categories</th>
<th>Categories</th>
<th>Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agriculture</td>
<td>Financial</td>
<td>Law Enforcement</td>
<td>SAFETY Act Information</td>
</tr>
<tr>
<td>Controlled Technical Information</td>
<td>Foreign Government Information</td>
<td>Legal</td>
<td>Statistical</td>
</tr>
<tr>
<td>Copyright</td>
<td>Geodetic Product Information</td>
<td>Nuclear</td>
<td></td>
</tr>
<tr>
<td>Critical Infrastructure</td>
<td>Immigration</td>
<td>Patent</td>
<td></td>
</tr>
<tr>
<td>Export Control</td>
<td>Information Systems</td>
<td>Privacy</td>
<td></td>
</tr>
<tr>
<td>Emergency Management</td>
<td>Intelligence</td>
<td>Proprietary Business Information</td>
<td></td>
</tr>
</tbody>
</table>
ALL FEDERAL AGENCIES AND THE DEPARTMENT OF DEFENSE

Safeguarding Covered Defense Information & Cyber Incident Reporting

Cyber Security

Basic Safeguarding of Covered Contractor Information Systems

DFARS Subpart 204.7 252.204-7012

FAR Subpart 4.19 52.204-21
FAR 52.204-21 BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS

Applicability
- On contracts/system with Federal Contract Information
- All federal contracts and subcontracts at any tier
- Exclusion - COTS products

Compliance
- Mandatory flow-down at all tiers
- Imposes 15 requirements that correlate to 17 NIST SP 800-171 security controls (limited subset)
- Suppliers agree to controls by signing the contract
DFARS 7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

Applicability:

- On contracts/systems where Covered Defense Information (CDI) resides or operationally critical support

- CDI identified by the Contracting Officer (CO), Prime Contractor, or higher tiered subcontractor

- CDI identified in Distribution Statement B-F & Section J of the contract & markings on the data sheets

- If in doubt ask, before you sign the contract
DFARS 7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (CONT.)

Compliance:

- Compliance = Implementation of NIST SP 800-171
- Implementation = self assessment + Systems Security Plan (SSP) & Plan Of Action And Milestones (POAM)
- An SSP to include a remediation plan is required for all controls not implemented by December 31, 2017
DFARS 7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (CONT.)

DFARS Key Points:

- No certification vendors

- Audit: There is no audit, this is only self attestation
DFARS 7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (CONT.)

Incident Reporting:
- Must report cyber incidents
- Upon discovery must conduct a review for evidence of compromise
- Report within 72 hours directly to DoD https://dibnet.dod.mil/portal/intranet/
- Must have a DoD approved medium Assurance Certificate
- Must provide DoD-assigned incident report number to prime/higher tiered subcontractor
- Must preserve and protect images of known affected images and systems for 90 days
- Must provide DoD access to additional information or equipment necessary to conduct forensics analysis
- Must submit any malicious software uncovered to DC3
252.204-7008  COMPLIANCE WITH SAFEGUARDING COVERED DEFENSE INFORMATION CONTROLS

Applicability:

In all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial items.

Exclusions: Except for solicitations solely for the acquisition of commercially available off-the-shelf (COTS) items.

Compliance:

By submission of this offer, the Offeror represents that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations” (see http://dx.doi.org/10.6028/NIST.SP.800-171) that are in effect at the time the solicitation is issued or as authorized by the contracting officer not later than December 31, 2017.
ADDITIONAL UPDATES

DoD draft guidance re: Cybersecurity requirements (April 2018)

The draft guidance includes: A matrix of NIST 800-171 requirements that contractors and DOD agencies should prioritize when implementing NIST 800-171, and several approaches for DOD agencies to evaluate NIST 800-171 implementation during the source selection process.
DANGERS OF NOT IMPLEMENTING FAR 52.204-21 AND DFARS 252.204-7012

*Businesses may not be able to do business with the government without having the proper security procedures in place in the future* – New DoD proposed Source Selection Changes.

Debarment – Put on the list of debarred companies excluded from Federal procurement and non-procurement programs throughout the U.S. Government.

Protest: Companies can file protests against the government for allowing companies to be awarded contracts who have not complied with FAR 52.204-21 and DFARS 252.204-7012
SUMMARY OF ASSESSMENTS PERFORMED
AGENDA

• Overview
• Control Evaluation
  • Most Commonly Missed 800-171 controls
• Our Process
  • Phase I
  • Phase II
  • Phase III
  • Phase IV
• Reporting
OVERVIEW

Throughout 2016-2018, H2L conducted assessments and identified 7012 Compliance of 52 national organizations.

H2L provided:
- Gap Analysis
- Plan of Actions and Milestones (POA&M)
- System Security Plans (SSP)
- Supporting Policies
- Vulnerability Assessments
CONTROL EVALUATION

Data was assessed and compiled based on the size of the organization.

Findings showed 6 distinct areas of weakness regardless of the company size.
MOST COMMONLY FAILED CONTROLS

1. 3.6.3 Incident Response Testing (35 instances)
2. 3.11.1 Risk Assessment (32 instances)
3. 3.3.6 Audit Reduction and Report Generation (31 instances)
4. 3.1.19 Access Control for Mobile Devices (30 instances)
5. 3.8.7 Media Use (30 instances)
6. 3.12.3 Continuous Monitoring (30 instances)
FAILED CONTROLS

Distribution of Failed Controls (All Organizations)
SMALL ORGANIZATIONS

Percentage of Failed Controls (Small-sized Organizations)
MEDIUM ORGANIZATIONS

Percentage of Failed Controls (Medium-sized Organizations)

Number of Control

Percentage

0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
LARGE ORGANIZATIONS

Percentage of Failed Controls (Large-sized Organizations)

NUMBER OF CONTROL
H2L SOLUTIONS’ ASSESSMENT: 4 PHASE APPROACH

Phase I: Gap Analysis

Phase II: SSP & Policy Development

Phase III: Vulnerability Assessment

Phase IV: VCISO & Continuing Services
PHASE I

- Interview and collection of artifacts
- Gap Analysis Report
- POA&M Generated
- Gap Analysis Report Generated
GAP ANALYSIS

We compile all of our findings into a report that is given to the client.

This report is used to generate the POA&M.
### PLAN OF ACTION & MILESTONES (POA&M)

<table>
<thead>
<tr>
<th>Weakness (1)</th>
<th>NIST Control (2)</th>
<th>POC (3)</th>
<th>Resources Required</th>
<th>Scheduled Completion Date</th>
<th>Milestones with Completion</th>
<th>Milestone Changes (1)</th>
<th>Source Identifying Weakness (6)</th>
<th>Status (9)</th>
<th>Comments (10)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IAAC-1 Impact High</td>
<td>JACFSO/HRUI</td>
<td>$50,000</td>
<td>5/30/2015</td>
<td>Develop an account management process - 05/01/2015; Management review of account management process 05/15/2015; Implement/Test account management process - 06/15/2015</td>
<td>Implementing and Testing the account management process delayed till 10/15/2015 due to inadequate funding</td>
<td>DFARS Baseline Assessment Conducted 10/11/2015</td>
<td>Ongoing</td>
<td>Funding will be available in FY 2006</td>
</tr>
<tr>
<td>2</td>
<td>Needs to employ the concept of least privilege, allowing only authorized access for access which are necessary to accomplish assigned tasks in accordance with mission and business functions</td>
<td>Configure devices with the least privilege necessary to perform the job, role, or function</td>
<td>AC-6</td>
<td>Least Privileges</td>
<td>DFARS Baseline Assessment Conducted 10/11/2015</td>
<td>Ongoing</td>
<td>Currently granting one admin rights to their department</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Needs to provide documentation, policy, or operating procedures demonstrating that the information system is configured to allow only authorized</td>
<td>AC-10 Wireless Access</td>
<td></td>
<td></td>
<td>DFARS Baseline Assessment Conducted 10/11/2015</td>
<td>Ongoing</td>
<td>Need to document in writing the process for authorized users connecting to WIFI</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
PHASE II: SSP & POLICIES

- Risk Assessment
- Incident Response
- Continuous Monitoring
- Access Control
- System Security Plan
- System and Information Integrity
- Media Protection
- Contingency Planning
- Audit and Accountability
The SSP follows guidance and requirements from **NIST SP 800-18**
The SSP details all information categorizing the company's security posture.

<table>
<thead>
<tr>
<th>ID</th>
<th>Control Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.89</td>
<td>Information System Backup</td>
<td>Partially Implemented</td>
</tr>
<tr>
<td>2.91</td>
<td>Personnel Screening</td>
<td>Partially Implemented</td>
</tr>
<tr>
<td>2.92</td>
<td>Personnel Termination and Transfer</td>
<td>Partially Implemented</td>
</tr>
<tr>
<td>3.10.1</td>
<td>Physical Access Authorizations</td>
<td>Partially Implemented</td>
</tr>
<tr>
<td>3.10.2</td>
<td>Monitoring Physical Access</td>
<td>Partially Implemented</td>
</tr>
<tr>
<td>3.10.3</td>
<td>Physical Access Control</td>
<td>Partially Implemented</td>
</tr>
<tr>
<td>3.10.4</td>
<td>Physical Access Control</td>
<td>Partially Implemented</td>
</tr>
<tr>
<td>3.10.5</td>
<td>Physical Access Control</td>
<td>Partially Implemented</td>
</tr>
<tr>
<td>3.10.6</td>
<td>Alternative Site</td>
<td>Partially Implemented</td>
</tr>
<tr>
<td>5.11.1</td>
<td>Risk Assessment</td>
<td>Not Implemented</td>
</tr>
<tr>
<td>5.11.2</td>
<td>Vulnerability Scanning</td>
<td>Not Implemented</td>
</tr>
<tr>
<td>5.11.3</td>
<td>Vulnerability Scanning</td>
<td>Not Implemented</td>
</tr>
</tbody>
</table>

1. **About this Document**
The System Security Plan (SSP) is designed to provide an overview of the security requirements of the system and describe the controls in place and planned for meeting those requirements. The SSP also defines responsibilities and expected behavior of all individuals who access the system.

This document and its accuracy are critical for system certification activity. For this reason, this SSP will be reviewed and updated, as necessary, at least annually. Documentation of each review and change made to the SSP will be captured in the Version History beginning on page 2 of this document. Items that should be included in the review are:

- Change in system architecture
- Change in system status
- Additional defense of system transmission
- Change in system access
- Change in certification and accreditation status

2. **Information System Name - Company**

Company is comprised of one executive system and does not contain any additional systems or major applications. This SSP provides an overview of the security requirements for the information system and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed, or stored by the system. Information security is an asset vital to our critical infrastructure and affects performance and protection is a key component of our organization. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed, or stored in the Company Information System.

The security safeguards implemented for the Company system meet the policy and control requirements set forth in this SSP. This system is subject to monitoring consistent with applicable laws, regulations, organizational policies, procedures and practices.

3. **Information System Owner**
The following individual is identified as the system owner or functional program/controls for the system.
AC POLICIES EXAMPLE

ACCESS CONTROL
POLICIES AND PRACTICES

1. PURPOSE
The purpose of this policy is to provide guidelines for establishing access control for H2L Solutions business systems.

2. SCOPE
The policies and practices defined herein apply to all H2L Solutions employees. This policy shall pertain to all staff according to their respective roles in conducting the business of the Corporation. Management shall conform to the policy regarding establishment, oversight, and implementation of these standards.

3. REFERENCES
   a) DFARS Clause 252.204-7012
   b) NIST SP 800-171 Rev1

4. DEFINITIONS
Access Control - The process of granting or denying specific requests to obtain and use information and related information processing services.
Least Privilege - The security objective of granting users only those accesses needed to perform their official duties.
Multi-factor Authentication - An approach to authentication that requires the presentation of two distinct kinds of evidence to authenticate and grant access. The usual kinds of evidence are something known and something possessed.
Session Lock - A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence. The session lock is implemented at the point where session activity can be determined. This is typically at the operating system level, but may be at the application-level. A session lock is not a substitute for logging out of the

6.1 ACCOUNT MANAGEMENT: 3.1.1, 3.1.2
Account Management
H2L Solutions shall identify account types (e.g., individual, group, system, application, guest/anonymous, and temporary) and establish conditions for group membership.
H2L Solutions shall identify authorized users of information system and specify access rights.
H2L Solutions shall establish a process to enforce access requests to be approved by assigned personnel (or a delegate) prior to provisioning user accounts.
H2L Solutions, [DEPARTMENT], shall notify [DEPARTMENT] to remove or deactivate access rights when users are terminated or transferred, or when access rights requirements change.
H2L Solutions shall remove, disable or rename default user accounts.
Access shall be granted based upon the principles of need-to-know, least-privilege, and separation of duties. Access not explicitly permitted shall be denied by default.
Access requests from users shall be recorded and follow the established H2L Solutions approval process.
Privileged accounts (e.g., system/network administrators having root level access, database administrators), shall only be allowed after approval by designated H2L Solutions personnel, assigned based on roles and will be controlled and monitored.
H2L Solutions shall implement processes to enforce [SPECIFY TIME] user access reviews performed by designated personnel or their assigned delegate(s)
H2L Solutions shall review information system accounts every [SPECIFY TIME] days.
H2L Solutions shall regulate information system access and define a process for security requirements for contractors, vendors, and other service providers.
PHASE III: VULNERABILITY ASSESSMENT

- **Internal and External Assessment Conducted**
- **Automated Scans for Identifying Attack Vectors**
- **Manual Verification to Uncover Potential Attack Avenues**
- **Executive and Technical Reports Generated**
PHASE IV: VCISO & CONTINUING CYBERSECURITY SERVICES

- Information security leadership and guidance
- Steering committee leadership or participation
- Security compliance management
- Security policy, process, and procedure development
- Security training and awareness
- Penetration testing
- Social engineering
- Vulnerability assessments
- Risk assessment
DFARS 252.204-7012 CYBER INCIDENT RESPONDING

The WHAT

- **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.
DFARS 252.204-7012 CYBER INCIDENT RESPONDING (CONT.)

The WHAT

- Assemble required list of reporting information.
- Save an image of the hard drive for 90 days.

The HOW

The WHEN

To report an incident, click on the “Report” button.

Access to this form requires a DoD-approved medium assurance External Certificate Authority (ECA) certificate. For information on obtaining a DoD-approved ECA certificate, please visit ECA website.

If you are unable to access this form, please call (877) 838-2174 or email: DCISE@DC3.mil.
Cyber Incidents must be reported within 72 hours.
Q&A AND FEEDBACK

Jonathan Hard
CEO & President
H2L Solutions, Inc.
jonathan.hard@h2lsolutions.com
1.256.679.9427
Holistic Approach to Securing Facility Related Control Systems

Ken Metzler
Holistic Approach to Securing Facility Related Control Systems

Agenda

• Why Secure a Facility Related Control System?
• Current State of Industrial Control Systems
• Managing Facility Related Control System Risk
• Command Roles in FRCS Security
Holistic Approach to Securing Facility Related Control Systems

Why Secure a (FRCS)?

• DoD’s buildings are vulnerable to cyber attacks
  – DoD has more than 300,000 buildings under its umbrella
• FRCSs, including air-gapped, are vulnerable.
  – Public Water Utility (2018): chemical mix changed for water tap supply; 2.5 million user records exposed
  – Water Treatment Plant (2018): control system network infected with cryptocurrency-mining malware
  – TRITON (2017): Attackers deploy new ICS attack framework “TRITON” and reprogram Safety Instrumented System controllers
  – Stuxnet (2010): targeted SCADA systems and is believed to have caused substantial damage to Iran's nuclear program
Current State of ICSs

• *CyberX Labs 2019 GLOBAL ICS & IIoT RISK REPORT*
  – ICSs continue to be soft targets for adversaries, with security gaps in key areas such as:
    • 53% of industrial sites have outdated Windows systems like XP
    • 69% have plain-text passwords traversing their control networks
    • 57% of sites are not running anti-virus protections that update signatures automatically
    • 16% have wireless access points
    • 84% of industrial sites of sites have at least one remotely accessible devices
  – **Bottom Line:** Cyber security state not much different from 2017 to 2018 except for a 23% decrease in deployed legacy Windows systems.
Holistic Approach to Securing Facility Related Control Systems

Command Roles in FRCS Security

• **Commander, Navy Installation Command (CNIC)**
  – Ultimately responsible for Cyber security of FRCSs

• **NAVFAC**
  – CNIC delegated Cyber execution of FRCSs to NAVFAC
  – NAVFAC CIO2/5 – RMF Authorizing Official and validation of FRCS security controls
  – NAVFAC CIO4s – CSPE FRCS connection and Navy Utility Monitoring Control System integration and support

• **Change Initiator**
  – Anyone who submits a request to create, change, or modify ANY FRCS
  – Collaborates with various team members to support FRCS Cyber security
Managing FRCS Risk

• Change & Configuration Management
  – Change & Configuration Board at each site and NAVFAC HQ to oversee FRCS changes
  – Enforces a set of standard processes and approved products
    • DoDIN Approved Product List – mandated by DoDI 8100.04
  – Provides value by:
    • Understanding the scope of potential cyberattack vectors
    • Identifying approved baseline configurations
    • Controlling changes within the environment
    • Continuously monitoring the status of identify unauthorized changes of components within a production environment
Managing FRCS Risk (cont.)

- **Cybersecurity in Contracting**
  - Utilizes Risk Management Framework process
  - Incorporate Cyber security at the beginning of building design
    - Cyber security after the fact significantly increases the cost and impacts the mission
  - Incorporates cybersecurity into control system design
    - Unified Facility Criteria 04-010-06
    - Unified Facility Guide Specifications 25 05 11
  - Military Construction Project Funding for Cyber
    - Cyber funding line item was introduced to MILCON 1391s in FY18
    - FY20 changes
      - Two distinct line items to account for contractor and government costs
Holistic Approach to Securing Facility Related Control Systems

Managing FRCS Risk (cont.)

• Control Systems Platform Enclave
  – DoD developed Enclave Boundary approach that provides Defense-In-Depth
  – Provides Risk Management Framework Continuous Monitoring service
  – IT systems managed by NAVFAC EURAFSWA CIO4 & FRCS by system owner
Questions?
References


3. Thomson, I. (2018, February 8). Now that’s taking the p... Sewage plant 'hacked' to craft crypto-coins. Retrieved from The Register: https://www.theregister.co.uk/2018/02/08/scada_hackers_cryptocurrencies/
