Legal Education Roundtable

Mary Beth Bosco, Partner
James D. Harris, Senior Counsel
Holland & Knight

April 4, 2017

THE NATIONAL CENTER FOR SIMULATION

Holland & Knight

Mary E. “Mary Beth” Bosco

Partner

Mary Beth Bosco has more than 30 years of experience working with new and experienced government contractors, and focuses her practice on advising such organizations in contract compliance, transactional matters and how to navigate the federal marketplace.

With a substantial background in regulatory matters and litigation, Ms. Bosco counsels companies on the drafting of procurement manuals and implementation of compliance and training programs, including reporting requirements as well as audits and procurement fraud investigations.

» **Contact Info**

» 202.469.5270

» MaryBeth.Bosco@hklaw.com

Practices

- Government Contracts
- Congressional Investigations
- False Claims Act Defense

Education

- George Washington University, J.D.
- Yale University, B.A.

James D. Harris

Senior Counsel

Jim Harris focuses his practice on securing the law for businesses needing access to national security information or state-owned minerals. Mr. Harris counsels executive officers, investors and lenders to some of the nation's leading companies in the defense and intelligence, and mining and energy sectors.

Mr. Harris provides intelligent advocacy for clients who must communicate with government officials presiding over highly discretionary federal programs. In addition, Mr. Harris provides actionable advice to clients who want a relationship of teamwork with federal regulators but demand regulatory nondiscrimination, accountability, proportionality and predictability for their business operations.

» **Contact Info**

» 202.828.1855

» James.Harris@hklaw.com

Practices

- International Trade
- Public Policy & Regulation
- Industrial Security

Education

- National Intelligence University, M.S.S.I.
- University of Houston, MBA
- University of Oklahoma, J.D.
- Southern Methodist University, B.B.A.

Compliance with Department of Defense Cybersecurity and Incident Reporting Requirements

Mary Beth Bosco

THE NATIONAL CENTER FOR SIMULATION

Holland & Knight

Overview

- **DFARS Final Rule**
- **DHS Proposed Rule/ATO**
- **NISPOM Changes/ATO**
- **Practice Pointers**

DoD Cybersecurity Rules: Basic Requirements

- Contractors storing or using "covered defense information" must provide "adequate security" for that information (DFARS Clause 252.204-7012).
- Mandatory 72-hour reporting requirement.
- No exceptions for small businesses; COTS items are excepted.
- Compliance deadline is 12/31/2017.
- Clauses must be flowed down to subcontractors **when covered defense information is necessary for performance of the subcontract.**

DoD Cybersecurity Rules: What information is covered?

» Covered Defense Information ("CDI")

- the information must be controlled (but unclassified) technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry) that requires safeguarding or dissemination controls 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 connection with 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.

DoD Cybersecurity Rules: What information is covered

- There are four categories of CDI:
  1. Controlled technical information;
  2. Critical information relating to the security of military operations;
  3. Export-controlled information; and
  4. “Any other information” subject to disclosure limitations.

DoD Cybersecurity Rules: Two Protection Levels

- If the contractor is operating a system or service on behalf of the government, then IT services and systems must meet specific requirements that will be set forth in the contract.
- Other contractor information systems supporting DoD contracts must meet the standards contained in National Institute of Standards and Technology (NIST) Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, or an "equally effective" system that must be approved *before award.*

DoD Cybersecurity Rules: NIST SP 800-171

- NIST 800-171 is organized around 14 “security families,” such as “Authentication and Identification.”
- Each family is assigned "Basic Security Requirements" and "Derived Security Requirements."
  - Basic Requirements are high-level standards.
  - Derived Requirements supplement Basic Requirements, and are based on the moderate baseline measures in NIST Pub. 800-53 (standards for federal information systems) as tailored to contractor information systems.
- December 30, 2015 Interim Rule delayed compliance date until December 31, 2017.

Current DoD Requirements: Mandatory Breach Requirements

- Covered contractors must report any cyber incidents within 72 hours of discovery.
- A cyber incident covers not just intrusions into information systems or data, but also circumstances that affect the contractor's ability to perform the requirements of a contract that is designated as operationally critical support.
- Reports submitted to the DoD-DIB Cyber Incident Reporting & Cyber Threat Information Sharing Portal, contractor needs a "DoD-approved medium assurance certificate" to report.

DoD Cloud Provider Standards

- External cloud service providers used in performance of a contract to store, process or transmit any covered defense information meet security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program Moderate baseline and comply with the cyber incident reporting obligations.

Department of Homeland Security Proposed Rules

- Proposed rules published on January 17, 2017.
- DHS is citing the “national security” exemption to the Administration’s regulatory freeze and “one for two” regulatory rule.
- Applies to CUI. But, DHS definition of CUI is slightly different than DoD and NARA.
  - “Controlled Unclassified Information (CUI)” is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.
  - Within the context of DHS, this includes such information which, if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy of individuals.

Broad Definition of Incident – Includes Policy Breach

- Definition of "Incident" does not require an actual compromise and includes a threat of a breach of policy
  - "Incident" means an occurrence that:
    - actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
    - constitutes a violation or *imminent threat of violation of law, security policies, security procedures, or acceptable use policies* [emphasis added].
    - All known or suspected incidents shall be reported to the Component Security Operations Center (SOC) in accordance with *4300A Sensitive Systems Handbook Attachment F Incident Response.* The Contractor shall also notify the Contracting Officer and COR using the contact information identified in the contract

DHS Proposed Regulations: Standards and ATOs

- Adequate security includes compliance with DHS policies and procedures in effect at the time of contract award. These policies and procedures are accessible at *http://www.dhs.gov/dhs-security-and-training-requirements-contractors*.
- *Authority to Operate.* Contractors operating Federal information systems, which include contractor information systems operating on behalf of the agency, must obtain Authority to Operate (ATO) which has been accepted and signed by the Component or Headquarters CIO, or designee.
- ATOs are valid for three years.
- An ATO is granted at the sole discretion of the Government and can be revoked at any time.
- To obtain an ATO, contractors must submit a Security Assessment Package, which must be validated by a third-party.

NISPOM

- **CHAPTER 8, INFORMATION SYSTEM *IS* SECURITY**
- Chapter 8, Section 1 (Page 8-1-1)

- Paragraph **8-100. General.**

  - Apply to all contractor classified systems.
  - 8-101. ISs Security Program. The contractor will maintain an ISs security program that incorporates a risk-based set of management, operational and technical controls, consistent with guidelines established by the CSA. The ISs security program must include, at a minimum, the following elements:

    a. Policies and procedures that reduce information security risks.

    b. Plans for providing adequate information security for data resident in the IS or on the networks, facilities or groups of ISs, as appropriate.

NISPOM

c. In addition to the training requirements outlined in paragraphs 3-107 and 3-108 of chapter 3 of this Manual, all IS authorized users will receive training on the security risks associated with their user activities and responsibilities under the NISP. The contractor will determine the appropriate content of the security training taking into consideration, assigned roles and responsibilities, specific security requirements, and the ISs to which personnel are authorized access.

d. Testing and evaluation of information security policies, procedures, practices, and security control implementation no less than annually to reflect a continuous monitoring approach of IS related risk assumptions and security control effectiveness.

e. A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices.

f. Procedures for detecting, reporting, and responding to security incidents and events.

g. Plans and procedures for ISs continuity of operations when required by contract.

h. A self-inspection program in accordance with paragraph 1-207b of chapter 1 of this Manual.

NISPOM Assessment and Authorization

- 8-201. Assessment. Security control assessment is a combined effort by the contractor and the CSA. The contractor will review, certify, and attest to the CSA that all systems have the appropriate protection measures in place. The CSA must receive the most complete, accurate, and trustworthy information to make timely, credible, and risk assessment based decisions on whether to authorize ISs operation.
- 8-202. Authorization. The AO, on behalf of the U.S. Government, will render an operational authorization decision based on the results of security assessment activities and the implementation of the CSA provided set of security controls. All ISs must be authorized before processing classified information.
  a. Interim Authorization to Operate (IATO). The AO may grant interim authorization (temporary authority) for an initial period up to 180 days with an option for the AO to extend the interim approval for an additional 180 days. The contractor will have the CSA-approved protection measures in place and functioning during the period of the IATO.
  b. ATO. The AO may grant an authorization to operate (ATO) following validation of the CSA-approved protection measures conducted during the IATO period, or may grant an ATO without an IATO period

Practice Pointers

- Don’t assume that the Trump Administration’s objective of reducing regulation will slow down or stop cyber regulation of government contractors.
  - The pressure on federal agencies to improve their own information security will flow down to contractors.
  - The distinctions between the standards imposed on contractors operating federal systems on behalf of the government and contractor systems housing government information are blurring.
  - But, because of the deregulation effort, contractors can expect to see more standards being set through agency guidance or agency manuals, as distinguished from formal rulemakings.
  - The “one for two” regulation rule contains an exception for regulations relating to national security. DHS, for example, considers its cybersecurity proposed rule to be exempt from the one for two rule.

Practice Pointers

- If you haven't done so already, update your information security policies to get ready for the December 31, 2017 deadline.
- Review your third-party agreements:
  - Do your standard subcontractor agreements meet the DoD and other flow-down requirements? Do they adequately protect you in the event of a breach?
  - Review consultant and independent contractor agreements to ensure they are aware of breach reporting requirements.
- Maintain a current inventory of what CUI is in your systems, where it is, who is the owner and what your contract requirements are.
- The December 2016 revision to NIST 800-171 requires a System Security Plan, which must "describe the boundary of [a contractor's] information system; the operational environment for the system; how the security requirements are implemented; and the relationships with or connections to other systems."
- If you are a DoD contractor, register to make sure you are ready to report to the DoD-DIB Cyber Incident Reporting & Cyber Threat Information Sharing Portal, because you need a "DoD-approved medium assurance certificate" to report.

Practice Pointers – You are a government contractor and you have a breach

- Conduct a review for evidence of compromise of CUI or CDI, 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 CDI or CUI covered defense information, *or that affect the Contractor's ability to provide operationally critical support*.
- Review contracts to identify reporting requirements – DoD has a 72-hour reporting requirement.
- *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 Office.
- *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 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.

Practice Pointers

- If all else fails… go back to paper.
  - We have heard from several smaller suppliers that this is what they are doing.

Effective Insider Threat Programs

James D. Harris

Holland & Knight

Purpose and History

- Insider Cases. String of insider cases occurring from 2009 to 2013, including Hasan, Manning, Snowden and Alexis.

- Structural Reforms Order. On October 7, 2011, the President issued Executive Order 13587, entitled "Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," which included tasking certain federal agencies to implement insider threat detection and prevention programs. See https://www.gpo.gov/fdsys/pkg/CFR-2012-title3-vol1/pdf/CFR-2012-title3-vol1-eo13587.pdf

- National Policy. On November 21, 2012, the President issued a Presidential Memorandum entitled, "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs." See https://www.ncsc.gov/nittf/docs/National_Insider_Threat_Policy.pdf

DSS Insider Threat Program: References

- NISPOM. On May 18, 2016, the Department of Defense ("DoD") DoD published Conforming Change 2 to the National Industrial Security Operating Manual ("NISPOM"). *See* http://dtic.mil/whs/directives/corres/pdf/522022M.pdf.

- ISL. On May 21, 2016, DSS posted additional information at DSS.mil, to include a relevant Industrial Security Letter — ISL 2016-02 (the "ISL"). *See* http://www.dss.mil/documents/isp/ISL2016-02.pdf.

- Plan Template. DSS has also published a Sample Insider Threat Program Plan (the "Plan Template"). *See* http://www.cdse.edu/documents/cdse/sample-insider-threat-program-plan-for-industry.pdf.

Seven Key Compliance Operations

- Establish a program (NISPOM paragraph 1.102a);
- Designate an Insider Threat Program Senior Official ("ITPSO") (NISPOM 1.102b);
- Self-inspect the program (NISPOM 1-207(b)(1));
- Train personnel (NISPOM 3-103(a and b));
- Keep records (NISPOM 3-103c);
- Monitor systems (NISPOM 8-100(d)); and
- Report information (NISPOM 1-300 *et seq.*).

Per ISL, "Program Plan" must have been established by November 30, 2016.

Minimum Objectives

DSS insider threat programs need to:

1. Detect
    a) Gather, integrate, and report relevant and credible information
    b) Are we asking the right questions? Looking at the right things?
    c) Who is in reporting and analysis chain?

2. Deter
    a) Training
    b) Audits, Supervision, Internal Controls

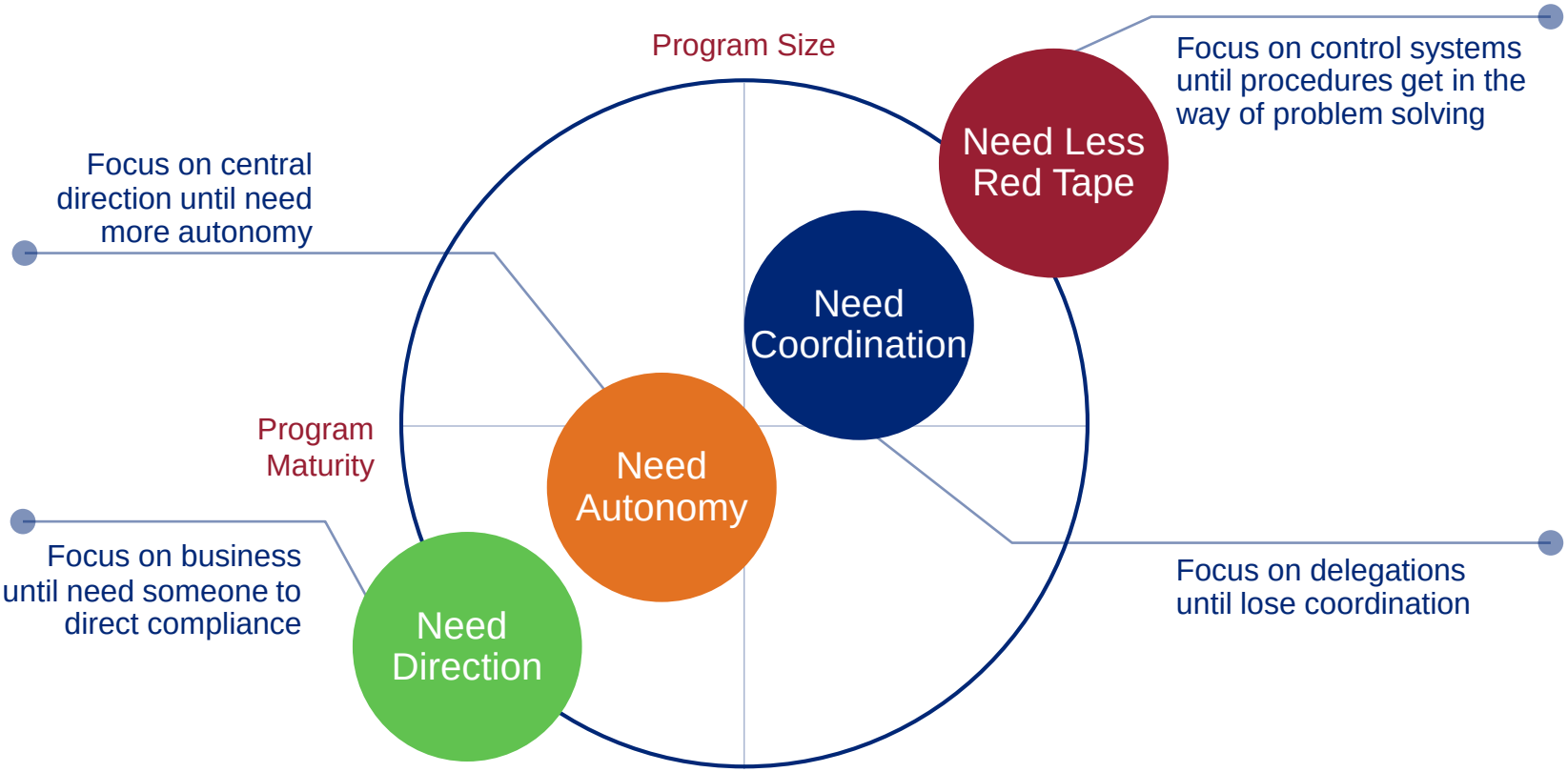
3. Mitigate
    a) Active defense
    b) Incident response

Impact on Business

1. How is the business...
   a) Managing things?
      i. *Well*… reliability, quality/fitness for intended use, property expectations.
      ii. *Bad*… stolen, broken, tampered, compromised.
   b) Leading people?
      i. *Well*… competent (complete tasks, achieve objectives, meet standards) and committed (to mission, colleagues, customers, etc.).
      ii. *Bad*… untrained, unqualified, questionable motivation and integrity, etc.
2. Will ITP fit into current management system as a…
   a) Bureaucratic overlay?
   b) Clandestine network?
   c) Integrated process?

Size and Complexity

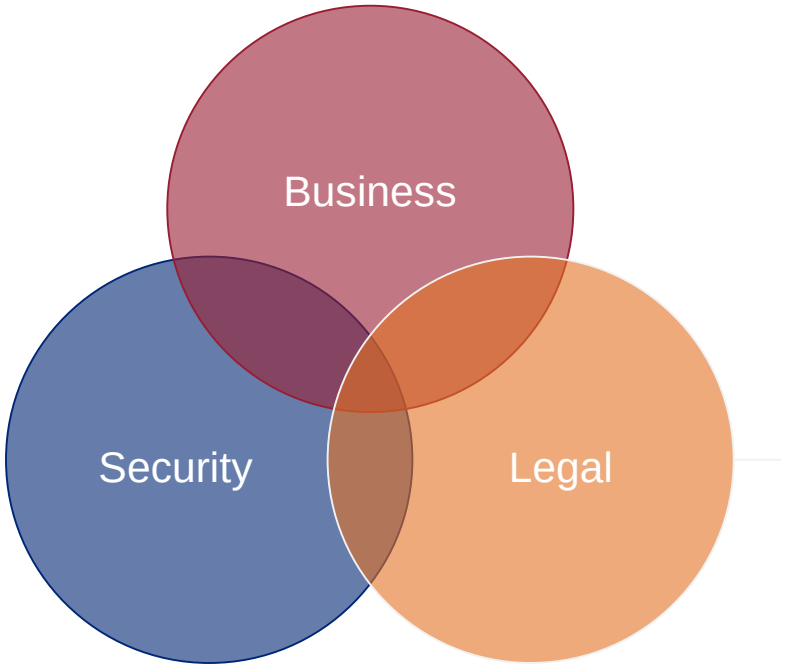
"DSS will consider the size and complexity of the cleared facility in assessing its implementation of an insider threat program to comply with NISPOM Change 2." – ISL



Stay in Sync

You will need leadership, teamwork and a helpful attitude to stay in synch on…

- What to look for
- What does it mean
- What to do
- How to do it



Best Practice Resources

» DSS

- ***Phases***: evaluation, formulation and implementation. *See* http://www.cdse.edu/itp-industry/documents/ITP-Best-Practices-Core-Elements.pdf.
- ***Core elements***: operations management & planning; gather; collaboration; education; protection specification; counterintelligence; monitoring; incident response; and audit & improvement. *See* http://www.cdse.edu/itp-industry/documents/ITP-Best-Practices-Core-Elements.pdf.

» Intelligence and National Security Alliance

- Preliminary Examination of Insider Threat programs in the U.S. Private Sector in September of 2013. *See* http://www.insaonline.org/i/d/a/Resources/InsiderThreat_WP.aspx.
- "*Road Map" for Insider Threat Programs. See* http://www.insaonline.org/InsiderThreat.

» CERT® Program of Carnegie Mellon University's Software Engineering Institute

- The Common Sense Guide to Mitigating Insider Threats. *See* http://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf.

Selected Best Practices: INSA

» Information

- Organizations must identify psychosocial events — anomalous, suspicious, or concerning nontechnical behaviors. A robust insider threat program integrates and analyzes ***technical and nontechnical indicators***.

» Organization

- An insider threat mitigation program cannot succeed without senior ***leadership support*** and involvement.
- An effective program requires a ***governance structure and solid partnerships*** with corporate Information Security, IT, Human Resources (HR), Public Relations, General Counsel, Ethics, Counterintelligence, Physical Security, and Executive Management involvement and engagement.

Selected Best Practices; CERT® Program

- What to do
  - Generally
    - Beginning with the hiring process, monitor and respond to ***suspicious or disruptive behavior***.
    - Anticipate and manage negative issues in ***the work environment***.
    - Clearly document and ***consistently enforce*** policies and controls.
    - Develop a comprehensive ***employee termination*** procedure.
  - Information Systems
    - Use a log correlation engine or security information and event management (SIEM) system to ***log, monitor and audit*** employee actions.
    - ***Establish a baseline*** of normal network device behavior.
    - Enforce ***separation of duties and least privilege***.
    - Institute ***stringent access controls and monitoring policies*** on privileged users.
    - Institutionalize ***system change controls***.
    - ***Close the doors*** to unauthorized data exfiltration.
    - Implement ***secure backup and recovery*** processes.

Consider Risk-based Responses

» Risk Elements

- Security risk is conventionally seen as a function of threat x vulnerability x consequence. If one factor is zero then risk is zero. Attack threats, cover vulnerabilities and recover from consequences. Realistic and rational response.

- When establishing an Insider Threat Program, assess each person in terms of ***all three risk elements***: threat, vulnerability and consequence characteristics. See Insider Threat in context of Human Resource Risk.

» Let Risk Guide Response

- Threats… coordinated plan of reporting and response most likely involving federal responders unless immediate action required to prevent loss.

- Vulnerabilities… training and awareness, human resource actions, reporting as necessary, privacy concerns.

- Consequences… to mission, assets, people if person becomes a threat or target (cost of repair or replace, redundancies, compartments, diversification).

THE NATIONAL CENTER FOR SIMULATION

Holland & Knight

Thank You!