SPACE & NAVAL WARFARE SYSTEMS COMMAND

Small Business Roundtable
Safeguarding Covered Defense Information

24 October 2018

Presented to:
SPAWAR Small Business Roundtable

Presented by:
CAPT Rick McCarthy, SPAWAR 2.0
Richard Jones, SPAWAR 6.0

Cybersecurity Landscape

Cyber threats targeting government unclassified information have dramatically increased

Cybersecurity incidents have surged 38% since 2014

The Global State of Information Security ® Survey 2016

Cyber attacks cost companies $400 billion every year

Inga Beale, CEO, Lloyds

Cybercrime will cost businesses over $2 trillion by 2019

Juniper Research

Impacts of successful attacks included downtime (46%), loss of revenue (28%), reputational damage (26%), and loss of customers (22%)

AT&T Cybersecurity Insights Vol. 4

61% of breach victims are businesses with <1,000 employees

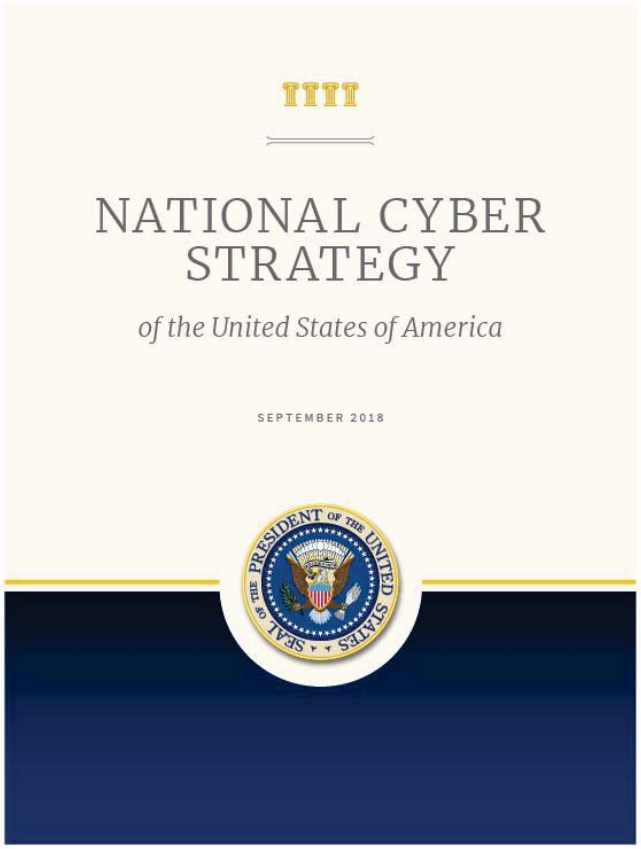
80% of breaches leverage stolen, weak, and/or guessable passwords

2017 Data Breach Investigations Report, Verizon

In a study of 200 corporate directors, 80% said that cyber security is discussed at most or all board meetings. However, two-thirds of CIOs and CISOs say senior leaders in their organization don't view cyber security as a strategic priority.

NYSE Governance Services and security vendor Veracode

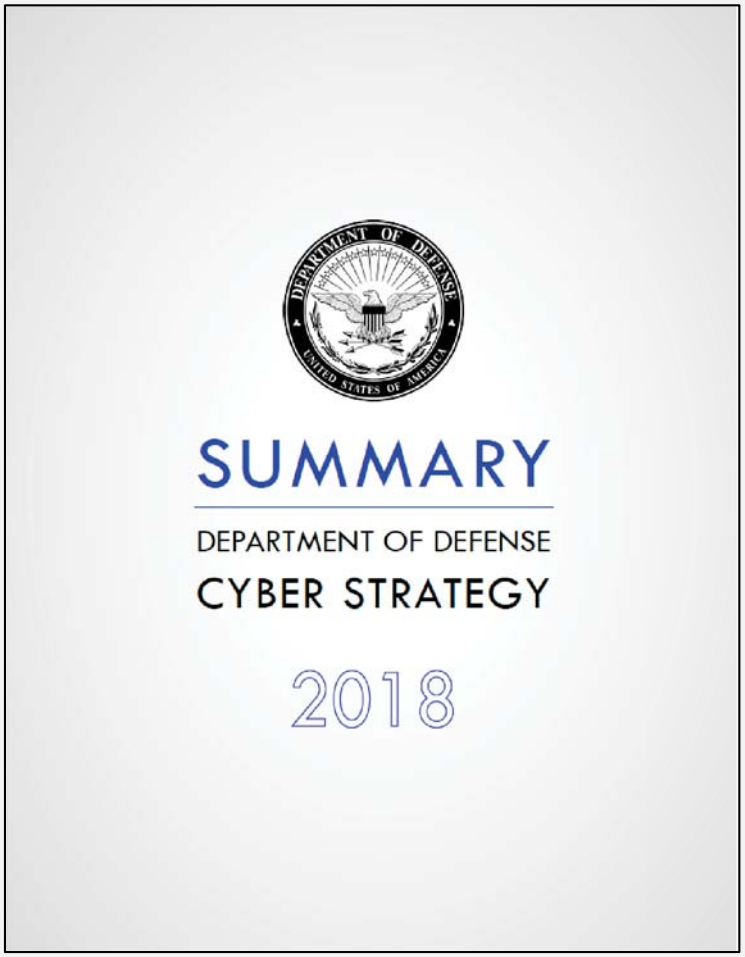
NATIONAL CYBER STRATEGY



STRENGTHEN FEDERAL CONTRACTOR CYBERSECURITY:

"The United States cannot afford to have sensitive government information or systems inadequately secured by contractors. Federal contractors provide important services to the United States Government and must properly secure the systems through which they provide those services. Going forward, the Federal Government will be able to assess the security of its data by reviewing contractor risk management practices and adequately testing, hunting, sensoring, and responding to incidents on contractor systems. Contracts with Federal departments and agencies will be drafted to authorize such activities for the purpose of improving cybersecurity. Among the acute concerns in this area are those contractors within the defense industrial base responsible for researching and developing key systems fielded by the DOD." (p. 7)

2018 DOD CYBER STRATEGY – THE PROBLEM



"The open, transnational, and decentralized nature of the Internet that we seek to protect creates significant vulnerabilities. Competitors deterred from engaging the United States and our allies in an armed conflict are using cyberspace operations to steal our technology, disrupt our government and commerce, challenge our democratic processes, and threaten our critical infrastructure." (p. 1)

DEFENDING CIVILIAN ASSETS

DEFENDING CIVILIAN ASSETS THAT ENABLE U.S. MILITARY ADVANTAGE

The Department must be prepared to defend non-DoD-owned Defense Critical Infrastructure (DCI) and Defense Industrial Base (DIB) networks and systems. Our chief goal in maintaining an ability to defend DCI is to ensure the infrastructure's continued functionality and ability to support DoD objectives in a contested cyber environment. Our focus working with DIB entities is to protect sensitive DoD information whose loss, either individually or in aggregate, could result in an erosion of Joint Force military advantage. As the Sector Specific Agency (SSA) for the DIB and a business partner with the DIB and DCI, the Department will: set and enforce standards for cybersecurity, resilience, and reporting; and be prepared, when requested and authorized, to provide direct assistance, including on non-DoD networks, prior to, during, and after an incident.

(p. 3)

EXISTENTIAL URGENCY

- Because We Missed a Shift!
  - Previous Models – Mat'l Locked / Safe!
  - New Model –
    - Information Readily Avail
    - Internet/Email - Attachments with Sensitive Artifacts
    - Covered Defense Information
      - CDI - Covered Technical Information ("CTI"); (2) operations security; (3) export controlled information; and (4) any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies.

EXISTENTIAL URGENCY

- Because We Missed a Shift!
  - Previous Models – Mat'l Locked / Safe!
  - New Model –
    - Information Readily Avail
    - Internet/Email - Attachments with Sensitive Artifacts
    - Covered Defense Information
      - CDI - Covered Technical Information ("CTI"); (2) operations security; (3) export controlled information; and (4) any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies.

"…we're in the cyber fight 24/7, 365 days a year, and our foes in that fight are sophisticated, and technologically advanced, and they are very well resourced, and they are focused on penetrating our systems."

– Adm. John Richardson

Chief of Naval Operations

What DoD Is Doing

DoD has a range of activities that include both regulatory and voluntary programs to improve the collective cybersecurity of the nation and protect U.S. interests:

- **Securing DoD's information systems and networks**
- **Codifying cybersecurity responsibilities and procedures for the acquisition workforce in defense acquisition policy**
  - **Contractual requirements implemented through the Federal Acquisition Regulation (FAR) and Defense FAR Supplement (DFARS)**
- **DoD's DIB Cybersecurity Program for voluntary cyber threat information sharing**
- **Leveraging security standards such as those identified in National Institute of Standards and Technology (NIST) Special Publication 800-171 "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" *(Revision 1 published Dec 2016)***

DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

DFARS Clause 252.204-7012 requires contractors/subcontractors to:

1. **Provide adequate security to safeguard covered defense information that resides on or is transiting through a contractor's internal information system or network**
2. **Report cyber incidents that affect a covered contractor information system or the covered defense information residing therein, or that affect the contractor's ability to perform requirements designated as operationally critical support**
3. **Submit malicious software discovered and isolated in connection with a reported cyber incident to the DoD Cyber Crime Center**
4. **If requested, submit media and additional information to support damage assessment**
5. **Flow down the clause in subcontracts for operationally critical support, or for which subcontract performance will involve covered defense information**

Contractor Compliance — Implementation of DFARS Clause 252.204-7012

- By signing the contract, the contractor agrees to comply with the terms of the contract and all requirements of the DFARS Clause 252.204-7012
- It is the contractor's responsibility to determine whether it is has implemented the NIST SP 800-171 (as well as any other security measures necessary to provide adequate security for covered defense information)
  - DoD will not certify that a contractor is compliant with the NIST SP 800-171 security requirements
  - Third party assessments or certifications of compliance are not required, authorized, or recognized by DoD

Adequate Security for Covered Defense Information

To provide adequate security to safeguard covered defense information:

DFARS 252.204-7012 (b) Adequate Security. … the contractor shall implement, at a minimum, the following information security protections:

****

(b)(2)(ii)(A): The contractor shall implement NIST SP 800-171, Protecting CUI in Nonfederal Systems and Organizations, as soon as practical, but not later than December 31, 2017

****

(b)(3): Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required

DFARS 252.204-7012 directs <u>how</u> the contractor shall protect covered defense information; The requirement <u>to</u> protect it is based in law, regulation, or Government wide policy.

Demonstrating Implementation of NIST SP 800-171 — System Security Plan and Plans of Action

- To document implementation of NIST SP 800-171, companies should have a system security plan in place, in addition to any associated plans of action:
  - Security Requirement 3.12.4 (System Security Plan): Requires the contractor to develop, document, and periodically update, system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems
  - Security Requirement 3.12.2 (Plans of Action): Requires the contractor to develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in their systems, and to describe how and when any unimplemented security requirements will be met
- Per NIST SP 800-171, Revision 1, Chapter 3: Federal agencies may consider the submitted system security plan and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether or not it is advisable to pursue an agreement or contract with the nonfederal organization

Implementing NIST SP 800-171 Security Requirements

Most requirements in NIST SP 800-171 are about policy, process, and configuring IT securely, but some may require security-related software or hardware. For companies new to the requirements, a reasonable approach would be to:

1. **Examine each of the requirements to determine**
   - **Policy or process requirements**
   - **Policy/process requirements that require an implementation in IT (typically by either configuring the IT in a certain way or through use of specific software)**
   - **IT configuration requirements**
   - **Any additional software or hardware required**

   The complexity of the company IT system may determine whether additional software or tools are required
2. **Determine which requirements can readily be accomplished by in-house IT personnel and which require additional research or assistance**
3. **Develop a plan of action and milestones to implement the requirements**

Alternative but Equally Effective Security Measures

See FAQ 59 - 62

- Per DFARS Clause 252.205-7012(b)(2)(ii)(B), if the offeror proposes to vary from NIST SP 800-171, the Offeror shall submit to the Contracting Officer, for consideration by the DoD CIO, a written explanation of -
  - Why security requirement is not applicable; OR
  - How an alternative but equally effective security measure is used to achieve equivalent protection
- When DoD CIO receives a request from a contracting officer, representatives in DoD CIO review the request to determine if the proposed alternative satisfies the security requirement, or if the requirement for non-applicability is acceptable
  - The assessment is documented and provided to the contracting officer, generally within 5 working days
  - If request is favorably adjudicated, the assessment should be included in the contractor's system security plan

SECURITY – FOURTH CRITICAL MEASURE

Deputy Secretary of Defense Patrick M. Shanahan

Shanahan: cybersecurity will become new measure for industry – article dated 19 Sep 2018

https://www.fifthdomain.com/digital-show-dailies/air-force-association/2018/09/19/shanahan-cyber-security-will-become-fourth-critical-measurement-for-industry/

"The Pentagon is preparing to press the defense industry to increase its cyber security … it will become a key measurement for how industry is judged by the department."

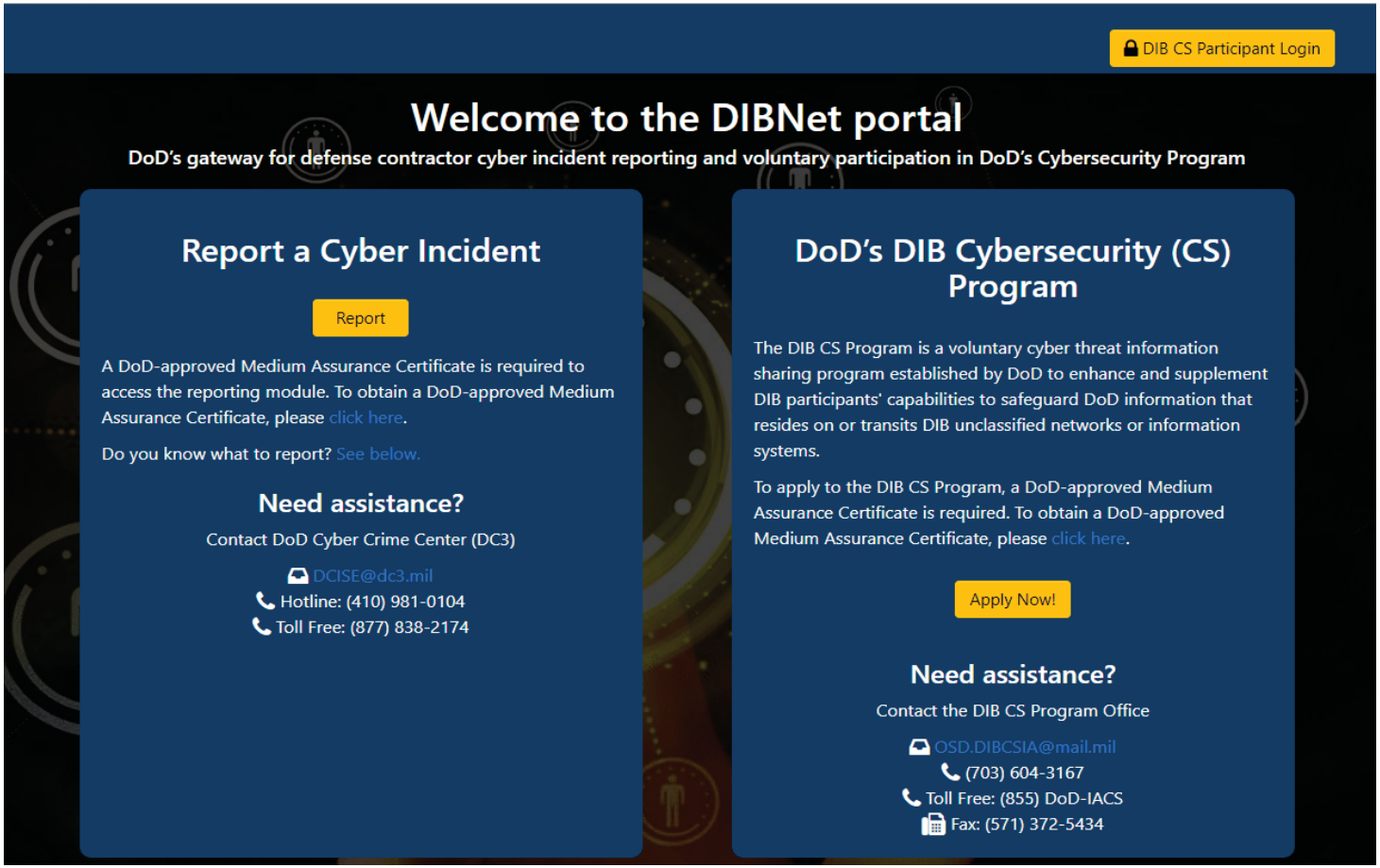
… "Cybersecurity is, you know, probably going to be what we call the 'fourth critical measurement.' We've got quality, cost, schedule, but security is one of those measures that we need to hold people accountable for."

…"We're going to work with our industrial partners to help them be as accountable for security as they are for quality."

…" The responsibilities of primes goes beyond just ensuring their own internal cyber security …laid down the gauntlet to the biggest industrial partners, saying flatly it is part of their job to make sure the lower-tier supplier are secure as well."

…"To try and address that, the Pentagon has been looking at a plan to launch red team cyber attacks on industrial partners, in which a cell would test vulnerabilities and try to penetrate the contractors' systems, in order to identify weaknesses."

DIB CS Web Portal



Access beyond this page requires a DoD-approved medium assurance certificate. For more information please visit the **ECA website**.

https://www.DIBNet.dod.mil

Administrative Oversight of DFARS Clause 252.204-7012

Additional Actions SPAWAR Pursuing in response to DFARS Clause 252.204-7012:

- **Encourage industry to adopt corporate, segment, or facility-level system security plans as may be appropriate in order to ensure more consistent implementations and to reduce costs**
- **Verify that system security plans and any associated plans of action are in place (assess plans against the NIST 800-171 requirements)**
- **If potential cybersecurity issue is detected –notify contractor, DoD program office, and DoD CIO**
- **Verify DFARS Clause 252.204-7012 is flowed down to sub-contractors/suppliers as appropriate**
- **For contracts awarded before October 2017 -verify that contractor submitted to DoD CIO notification of security requirements not yet implemented**
- **Verify contractor possesses DoD-approved medium assurance certificate to report cyber incidents**
- **When required, facilitate entry of government assessment team into contractor facilities via coordination with cognizant government and contractor stakeholders**

Resources

- NIST Manufacturing Extension Partnership (MEP)
  - Public-private partnership with Centers in all 50 states and Puerto Rico dedicated to serving small and medium-sized manufacturers
  - Published "Cybersecurity Self-Assessment Workbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements", November 2017

  https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf
- Procurement Technical Assistance Program (PTAP) and Procurement Technical Assistance Centers (PTACs)
  - Nationwide network of centers/counselors experienced in government contracting, many of which are affiliated with Small Business Development Centers and other small business programs

  http://www.dla.mil/HQ/SmallBusiness/PTAP.aspx
- Cybersecurity Evaluation Tool (CSET)
  - No-cost application, developed by DHS, provides step-by-step process to evaluate information technology network security practices

  https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET

Resources

- Cybersecurity in DoD Acquisition Regulations page at *(http://dodprocurementtoolbox.com/)* for Related Regulations, Policy, Frequently Asked Questions, and Resources, *June 26, 2017*
- DPAP Website (http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html) for DFARS, Procedures, Guidance and Information (PGI), and Frequently Asked Questions
- NIST SP 800-171, Revision 1 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf)
- Cloud Computing Security Requirements Guide (SRG) (http://iasecontent.disa.mil/cloud/SRG/)
- DoD's Defense Industrial Base Cybersecurity program (DIB CS Program) (https://dibnet.dod.mil)

Questions? Submit via email at osd.dibcsia@mail.mil

Additional Resources

- The California Advanced Supply Chain Analysis and Diversification Effort (CASCADE)
  http://business.ca.gov/CASCADE