NDIA

Defense Industrial Base IT and Cybersecurity Survey

Demographics

*Which of the following best describes your role at your organization?

○ C-Suite or Senior Leadership

○ IT Personnel

○ Cybersecurity Personnel

○ Other (Please specify)

Firmographics

*What is your organization's contractual relationship to the DoD? (Please check all that apply)

□ Only a prime contractor

□ Predominantly a prime contractor but also a subcontractor for a relatively few contracts

□ Predominantly a subcontractor but also a prime contractor for a relatively few contracts

□ Only a subcontractor

□ Unknown

How long has your organization served as either the prime contractor or as a subcontractor on a DoD contract?

○ 0-1yr

○ 1yr-5yrs

○ 5yrs - 10yrs

○ Over 10yrs

○ Unknown

What are your primary and secondary North American Industry Classification System (NAICS) codes? (Please check all that apply)

□ 3329: Other Fabricated Metal Product Manufacturing

□ 3342: Communications Equipment Manufacturing

□ 3344: Semiconductor and Other Electronic Component Manufacturing

□ 3345: Navigational, Measuring, Electromedical, and Control Instruments Manufacturing

□ 3359: Other Electrical Equipment and Component Manufacturing

□ 3364: Aerospace Product and Parts Manufacturing

□ 5415: Computer Systems Design and Related Services

□ 5417: Scientific Research and Development Services

□ Unknown

□ Other NAICS 4-digit code (Please specify as Primary or Secondary):

□

*How many employees are in your organization?

○ 1 - 49 employees
○ 50 - 99 employees
○ 100 - 249 employees
○ 250 - 499 employees
○ 500 - 999 employees
○ 1,000-2,499 employees
○ 2,500-4,999 employees
○ 5000 or more employees

*What was your organization's total annual revenue in the last year?

○ Less than $1M
○ $1M - $5M
○ $5M - $10M
○ $10M - $50M
○ $50M - $100M
○ $100M - $250M
○ $250M - $500M
○ $500M - $1B
○ More than $1B

IT and Cybersecurity

*Please check all that apply to your organization’s Information Technology (IT) environment used in support of DoD:

□ Organization Owned: My organization owns and operates our IT environment(s)

□ Commercial Cloud Environment(s) which is FedRAMP authorized:

□ Commercial Cloud Environment(s) which meet DoD Cloud Computing Security Requirements Guide (SRG) for a particular Impact Level:

□ Commercial Cloud Environment(s) which are not FedRAMP authorized or do not meet DoD SRG requirements

□ Managed Service Provider (MSP) Provided Environments: My organization uses an environment provided by my MSP, which in turn may leverage a commercial cloud or other environment.

□ Partner Provided Environments: IT resources provided by another partner such as prime or sub-contractor

□ Government Equipment: IT which is Government Furnished Equipment (GFE)

□ Government Environment(s): Government provided IT environment(s)

□ OT Environment: Operational Technology environments in addition to Information Technology

□ Other (Please specify)

Please provide further information about your Commercial Cloud Environment(s) or Government Environment(s), if available

Specify Provider(s) of Commercial Cloud Environment(s) that are FedRAMP authorized:	
FedRAMP Baseline (Low, Moderate or High):	
Specify Provider(s) of Commercial Cloud Environment(s) that meet DoD Cloud Computing Security Requirements Guide (SRG):	
DoD Cloud Computing SRG Impact Level:	
Specify Government Environment(s):	

*Who manages and supports your organization’s IT environment? Who manages and/or supports your organization’s cybersecurity? (Please check all that apply)

□ Employee(s) within organization

□ Managed Service Provider (MSP) (e.g., service providers who may have responsibilities related to IT and perhaps some cybersecurity)

□ Managed Security Service Provider (MSSP) (e.g., service providers who may focus on cybersecurity)

□ External party (other than an MSP or MSSP)

□ Not sure

□ Other (Please specify)

*How many internal employees are dedicated to managing or supporting your organization’s IT and cybersecurity? (Scroll bar for more answer options.)

Number of employees who manage or support IT

○ 0

○ < 1 full time equivalent (FTE)

○ 1-2 FTEs

○ 2-5 FTEs

○ 5-10 FTEs

○ 10-20 FTEs

○ More than 20 FTEs

○ Unknown

Number of employees who manage or support cybersecurity (i.e. in addition to those who manage or support IT)

○ 0

○ < 1 full time equivalent (FTE)

○ 1-2 FTEs

○ 2-5 FTEs

○ 5-10 FTEs

○ 10-20 FTEs

○ More than 20 FTEs

○ Unknown

*What percentage of your organization’s annual revenue is currently allocated towards spending on IT?

○ Less than 5% ○ 5-10% ○ 10-15%

○ More than 15% ○ Unknown

*What percentage of your organization’s annual revenue is currently allocated towards spending on cybersecurity spending?

○ No allocation

○ 0%-0.5%

○ 0.5%-1%

○ 1%-2%

○ 2%-4%

○ More than 4%

○ Unknown

Cybersecurity: Compliance, Challenges, Awareness

* In support of DoD contract(s), do you currently process, store, or transmit controlled unclassified information (CUI)?

○ Yes ○ No ○ Not Sure

For which of the following IT (Information Technology) and/or OT (Operational Technology) environments does your organization process, store, or transmit Controlled Unclassified Information (CUI)? (Please check all that apply)

- □ Network (owned by organization) - Includes internal networks and systems
- □ Network enclave for CUI (owned by organization) - Dedicated network segment for CUI
- □ Cloud IaaS, PaaS, and SaaS - Infrastructure, Platform, and Software as a Service in the cloud
- □ Cloud-based CUI enclave - Secure cloud environment specifically for CUI
- □ OT - Operational technology systems, such as industrial control systems
- □ Other environments (please specify)
- □ Not sure

When working with CUI data, indicate the type of environment your business requires: (check all that applies)

- □ An environment allowing for document or information exchange between organizations
- □ An environment which supports software development, data analysis and testing
- □ An environment which offers an appropriate means to download and/or transfer data from the environment (e.g., needing to download designs offline to process such as 3D print models)
- □ An environment which offers the ability to communicate with mobile devices
- □ An environment which offers high-performance computing capabilities
- □ Other (Please specify)

□

*Which of the following activities related to NIST SP 800-171 self-assessments and/or independent assessments have your organization conducted or supported? (Please check all that apply)

□ Self-assessment

□ Reporting of self-assessment to SPRS

□ Supported an independent, third-party assessment

□ Supported a DCMA DIBCAC Medium Assessment

□ Supported a DCMA DIBCAC High Assessment

□ No self-assessments

□ No independent (DoD or third-party) assessment

□ Unknown

*What is your most recent NIST SP 800-171 assessment score?

○ 110

○ 88-109

○ 0-87

○ < 0

○ Not sure

*What is the source of your most recent NIST SP 800-171 assessment score?

○ Self assessment

○ Third party assessment

○ DCMA DIBCAC

○ Not sure

If you have not fully implemented all NIST SP 800-171 security requirements, how much time do you think will be needed to address any remaining items based on your Plan(s) of Actions and Milestones (POA&M(s))?

○ < 6 months

○ 6-12 months

○ 1-2 years

○ More than 2 years

○ Not sure

*If your organization uses external IT/cybersecurity support services (like MSPs, MSSPs), have these providers supplied documentation detailing shared and sole responsibilities for NIST SP 800-171 self-assessments or independent assessments? (Please check all that apply)

- □ Yes, received a complete shared responsibility matrix for all 110 security requirements in NIST SP 800-171.
- □ Yes, received a complete shared responsibility matrix for all 320 assessment objectives in NIST SP 800-171A.
- □ Received partial documentation for NIST SP 800-171 or 800-171A requirements/objectives.
- □ No, did not receive a shared responsibility matrix for NIST SP 800-171 requirements.
- □ No, did not receive a shared responsibility matrix for NIST SP 800-171A objectives.
- □ Not applicable – We do not use external IT/cybersecurity support services.
- □ Unknown

Based on your organization's progress to date, what is your organization's estimate for the total non-recurring cost to implement all of the 110 security requirements specified in NIST SP 800-171? Total recurring annual cost?* Please exclude costs associated with assessments. (Scroll bar for more answer options.)

Non-recurring cost estimate

○ < $50K

○ $50K - $100K

○ $100K - $250K

○ $250K - $500K

○ $500K - $1M

○ $1M - $2M

○ $2M - $5M

○ More than $5M

○ Not sure

Recurring annual cost estimate

○ < $50K

○ $50K - $100K

○ $100K - $250K

○ $250K - $500K

○ $500K - $1M

○ $1M - $2M

○ $2M - $5M

○ More than $5M

○ Not sure

*Which of the following are challenges that your organization faces in implementing the security requirements in NIST SP 800-171? (Please check all that apply)

□ Difficulty in understanding the security requirements in NIST SP 800-171

□ Insufficient guidance on NIST SP 800-171 compliance

□ Financial cost associated with implementing NIST SP 800-171

□ Shortage of qualified IT professionals

□ Difficulty in identifying qualified MSPs and comparing costs and services

□ Shortage of qualified cybersecurity professionals

□ Difficulty in identifying qualified MSSPs and comparing costs and services

□ Difficulty in achieving consensus or support among key decision-makers within organization for implementation

□ Uncertainty about the location of CUI within our systems and how to effectively protect it

□ Other (Please specify)

*Are you aware of DoD Cybersecurity-as-a-Service (CSaaS) offerings from various DoD Components such as the DoD Cyber Crime Center (DC3) and NSA, which are available to DIB contractors (in some cases, under certain criteria)?

○ No

○ Somewhat familiar

○ Yes, familiar and are currently using one or more of these offerings

○ Yes, familiar and currently not leveraging these offerings

○ Yes, familiar but unable to utilize

Do you voluntarily use one of the following DoD CSaaS offerings? (Please check all that apply)

□ DC3 DCISE: DCISE Cubed

□ DC3 DCISE: Cyber Resilience Analysis (CRA)

□ DC3 DCISE: Adversary Emulation

□ NSA Cybersecurity Collaboration Center: Protective Domain Name System (PDNS)

□ NSA Cybersecurity Collaboration Center: Attack Surface Management

□ NSA Cybersecurity Collaboration Center: Threat Intelligence Collaboration

□ United States Air Force: Blue Cyber Initiative

□ DoD Office of Small Business Programs: Project Spectrum

□ Other (Please specify)

What are possible impediments to your organization leveraging one or more DoD CSaaS offerings? (Please check all that apply)

□ Not aware of offerings

□ Time to learn about the service, sign agreement, and support initiation of service

□ Lack of IT/cybersecurity support

□ Coordination with Managed Service Provider and associated costs

□ Coordination with Managed Security Service Provider and associated costs

□ Concerns about trust and/or confidentiality

□ Offerings do not address gaps or needs in organization's cybersecurity

□ Other (Please specify)