

NDIA Cybersecurity Survey Interim Results

Assessing awareness, readiness and willingness to
comply with:

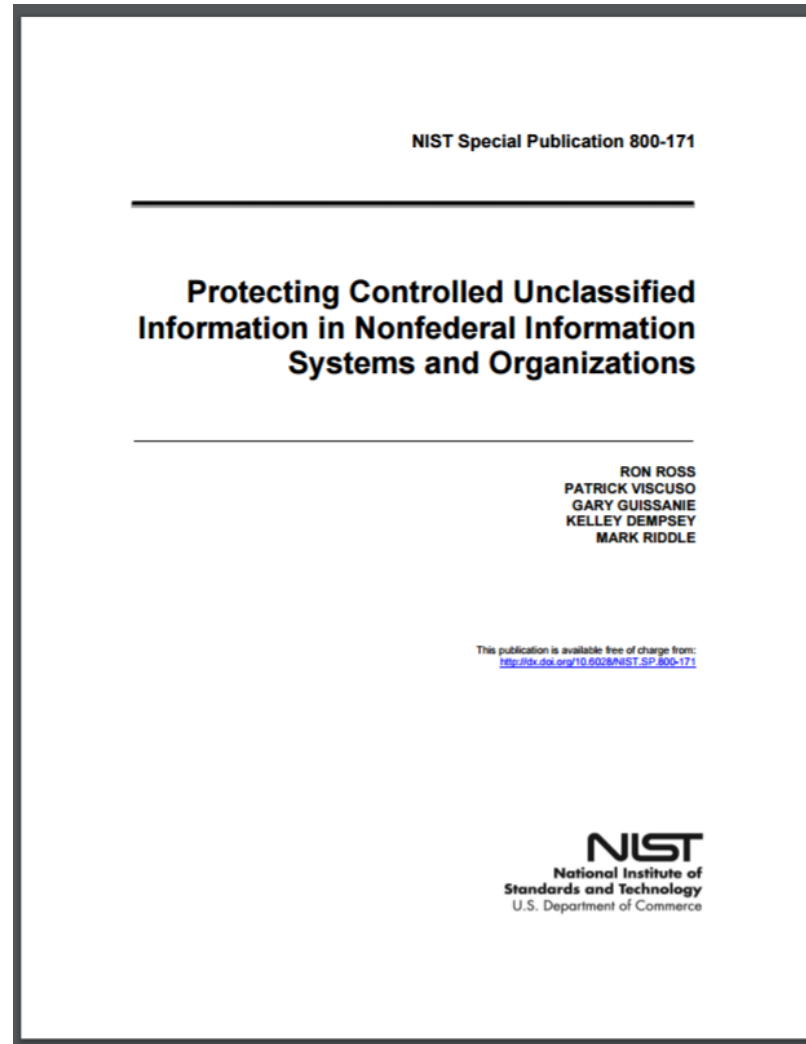
48 CFR 252.204-7012

Safeguarding Covered Defense Information and Cyber
Incident Reporting

**Manufacturing Division
June 2017**


NIST 800-171

- **Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations**
- **DFARS 252.204-7012**
- **December 2017 Compliance Requirement**




Plenty of Help...

NDIA



Safeguarding of Unclassified Controlled Technical Information (UCTI)

Understanding and Complying with the Defense Federal Acquisition Regulation Supplement Clause 252.204-7012



DFARS Cybersecurity Regulations
Your DFARS NIST SP 800-171 Roadmap to **Success**

[Download Roadmap >](#)

NATIONAL CONTRACT MANAGEMENT ASSOCIATION

DFARS 252.204-7012 (Sept 2015)

"Safeguarding Covered Defense Information and Cyber Incident Reporting": INTERIM RULE:

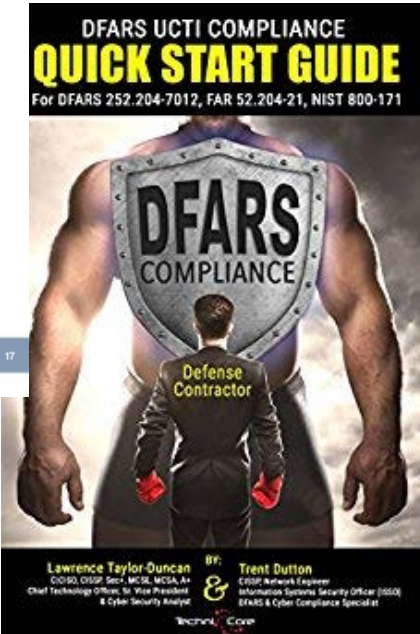
- 1) 72 Hr Network Penetration Reporting
- 2) Contracting for Cloud Services

Four Recommended Contractor Actions:

- 1) Register with DOD to obtain a mandatory Medium Assurance certificate
- 2) Identify & Mark all Attributional/Proprietary Information
- 3) SCM Flowdown to Subcontractors (including Commercial Item and Small Business Subcontracts, Teaming Agreements etc). Sub must report to Prime and DOD within 72 hrs (no Tier limitation).
- 4) Monitor Existing Contract Mods



Business Success Through Contract Management Excellence



DFARS UCTI COMPLIANCE QUICK START GUIDE
For DFARS 252.204-7012, FAR 52.204-21, NIST 800-171

DFARS COMPLIANCE

Defense Contractor

Lawrence Taylor-Duncan
CISO, CISSP, JNCI, MCSE, MCSA, A+
Chief Technology Officer, Sr. Vice President
& Cyber Security Analyst

By: Trent Dutton
CISSP, Network Engineer
Information Systems Security Officer (ISSO)
& Cyber Security Analyst & Cyber Compliance Specialist

Techni Case

**31
DEC
17**

Controlled Unclassified Information (CUI)
Compliance

Are you ready?

...But How Ready Are We?

NDIA

NDIA Cyber Security Survey 2017

Q1 NDIA-Michigan State University Study: Cyber Security Survey 2017 The risk from cybersecurity threats is growing, particularly for those in the defense industry. The National Defense Industrial Association (NDIA) Manufacturing Division, in conjunction with Michigan State University, is interested in getting a sense of your awareness and opinion on this important topic. Attached is a survey that will help us identify and address key issues that will impact organizations like yours. As a senior manager in such a firm, you are being asked to spend about 10 minutes of your time in completing this important survey. Michigan State University is conducting this survey on behalf of the NDIA and will deliver only aggregate data. Your private company data will remain confidential. Furthermore, please understand that your participation in this study is entirely voluntary; you are not required to answer any and all questions (however, it would greatly enhance the usefulness of the survey if you are able to answer all of the questions posed). Should you have any questions regarding the items in this survey, please call Steven A. Meinyk at (517) 432-6410 or by email at meinyk@msu.edu. Thank you for your participation.

Q2 Please include your willingness to participate in this study by selecting the appropriate response from the options found below.

- Yes, I would like to participate. (1)
- No, I would not like to participate. (2)

Condition: No, I would not like to par... is Selected. Skip To: End of Survey.



MICHIGAN STATE
UNIVERSITY

NDIA

National Defense Industrial Association

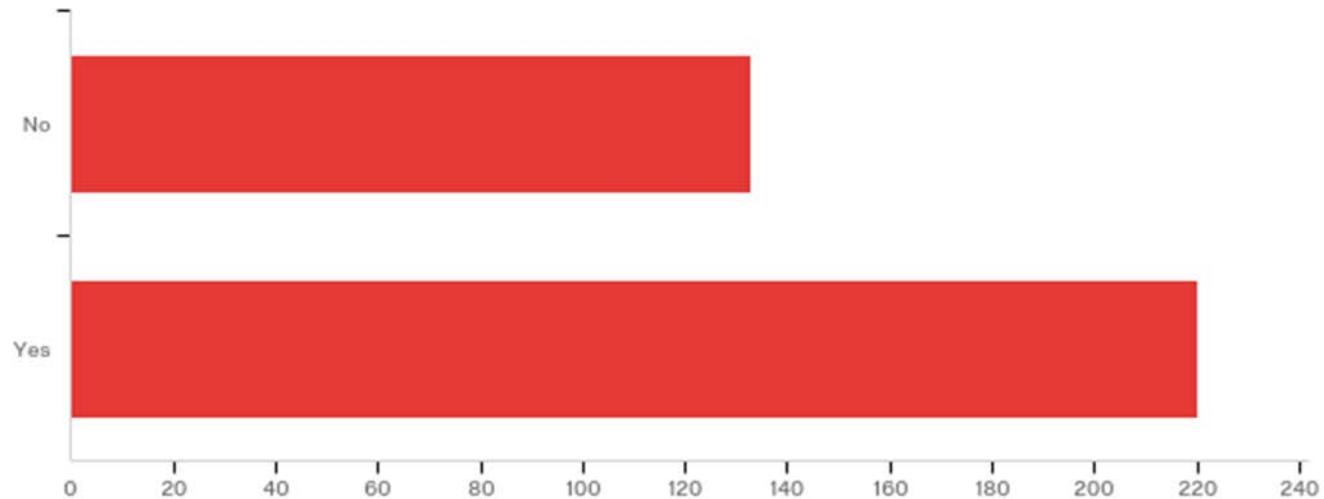
2017 NDIA CyberSecurity Survey



- **Created on March 20 2017 to assess awareness and current progress on meeting new DOD cyber security requirements.**
- **Distributed to NDIA list**
- **Response**
 - 401 accesses
 - 382 – willing to participate
 - 13 – did not want to participate
- **Suppliers**
 - 134 – No (37%)
 - 227 – Yes (63%)

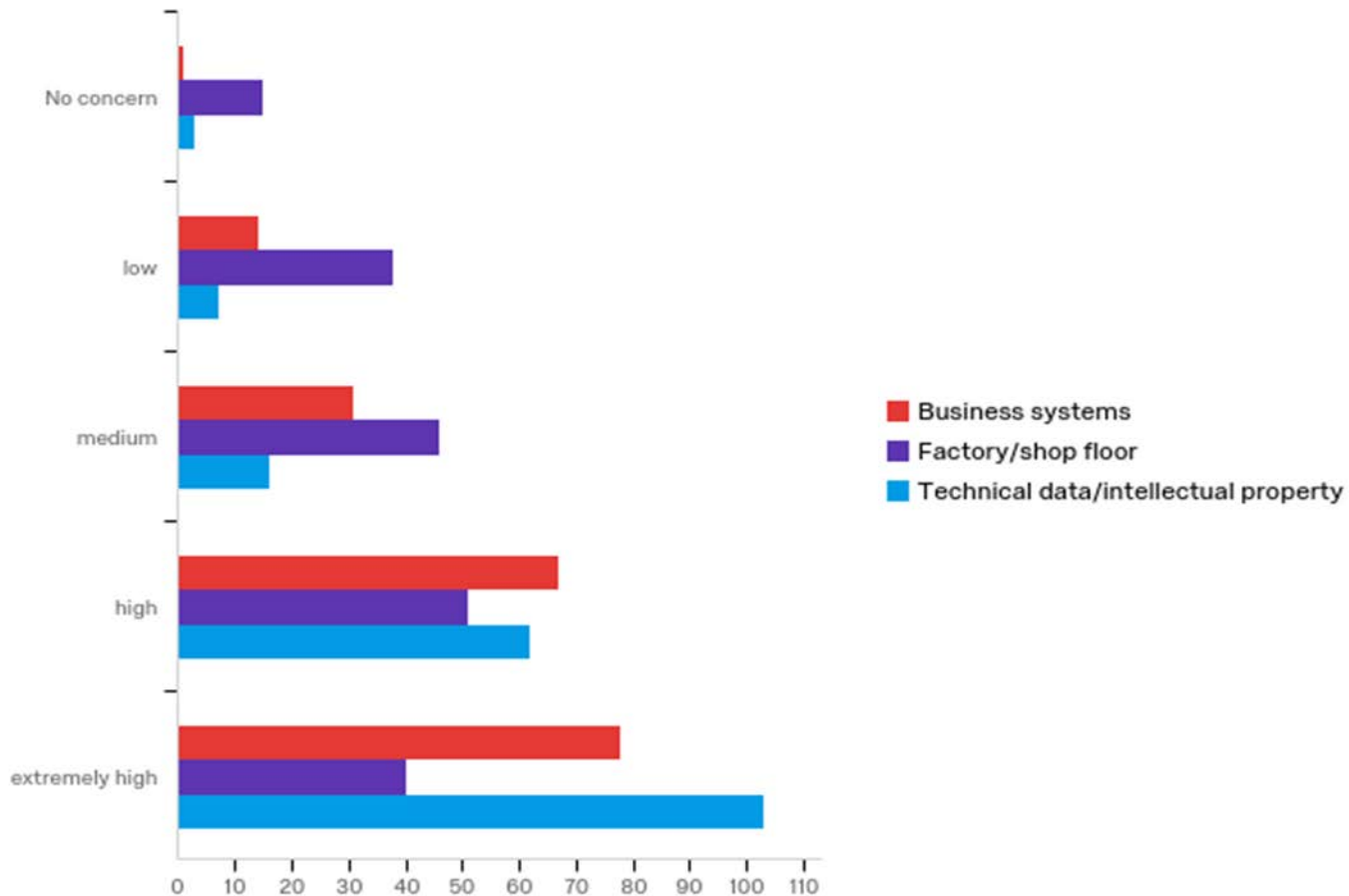
220 Qualified Respondants

Q3 - Does your organization manufacture parts, components, systems or supplies that are used either directly or indirectly by the Department of Defense (DOD)?



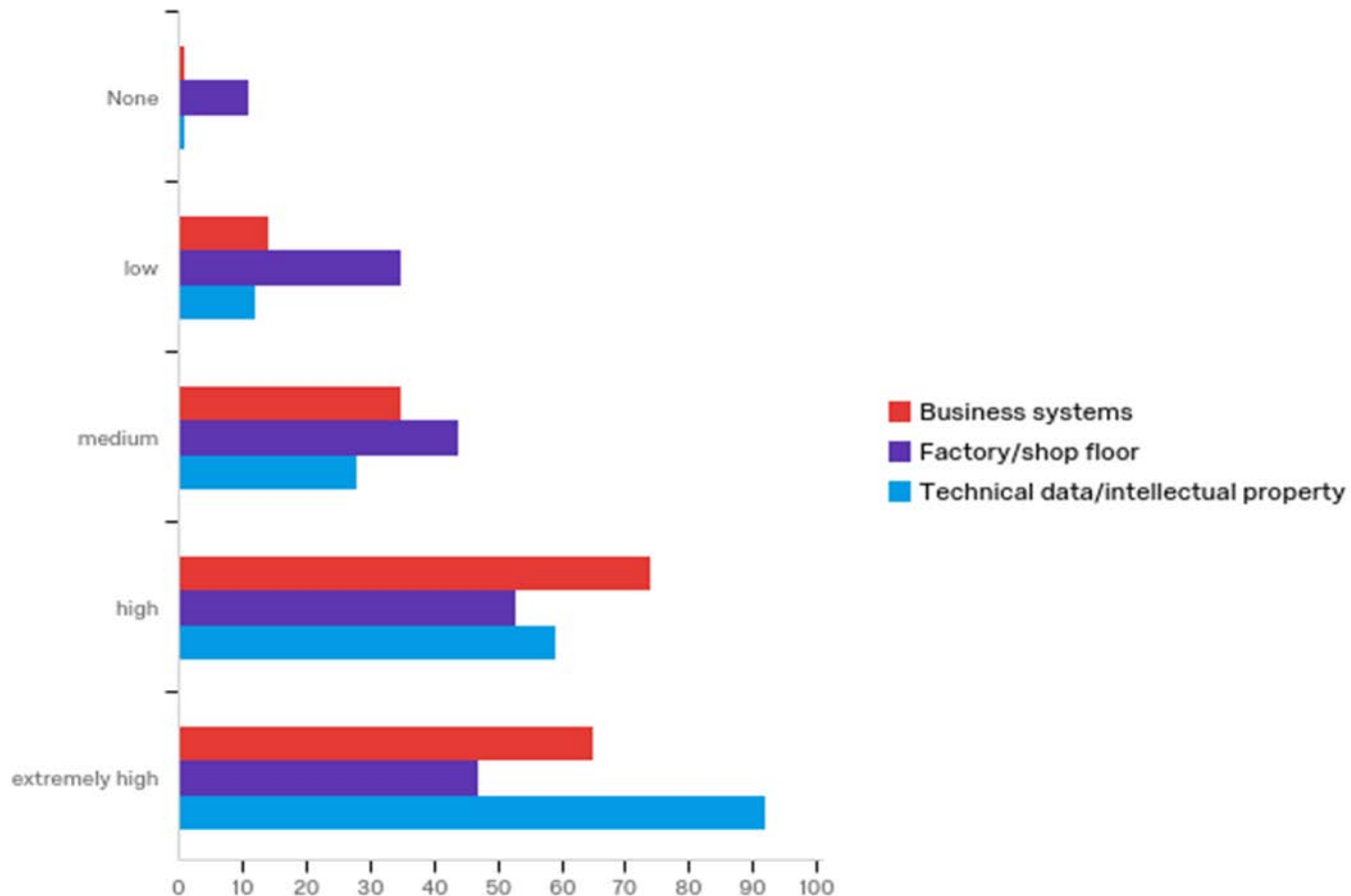
Threat Concern Runs High

Q5 - How concerned are you with cyber security threats to your firm?



And Some Have Taken Action

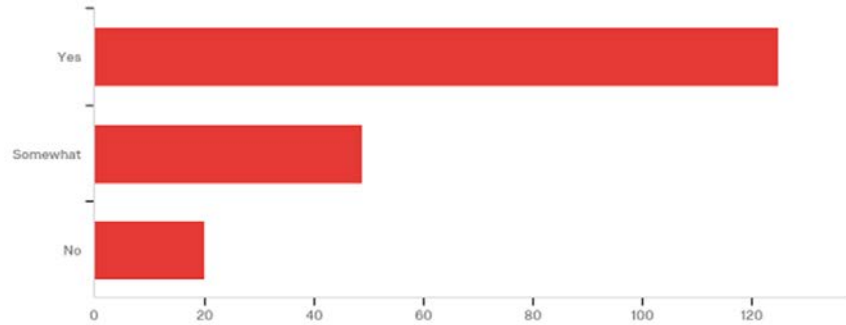
Q6 - How much effort has your firm put into providing protection against cyber security threats to your firm?



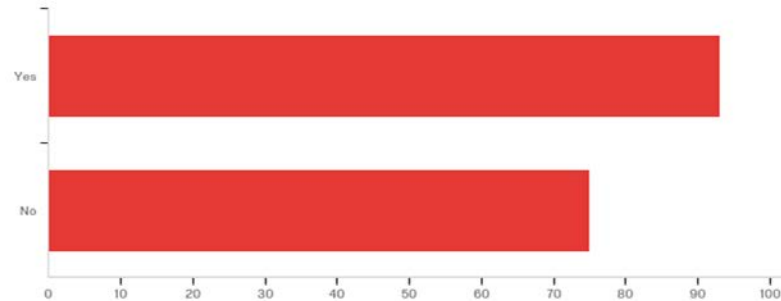
- **Currently focused primarily on business systems and technical data**
 - Average focus on business system investment (out of 5 where 5 is extremely high and 1 is no concern)
 - 4/5
 - Average focus on technical data
 - 4.2/5
 - Average investment focus on shop floor systems
 - Less emphasis
 - Mean – 3.4/5

Awareness is High

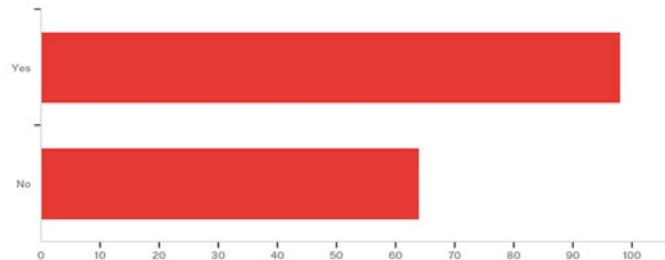
Q7 - Are you aware of the mandatory Defense Federal Acquisition Regulations Supplement (DFARS) clause now being included in some contracts to address "Safeguarding covered defense information and cyber incident reporting?" (DFARS 252.204-7012, which references NIST 800-171)?



Q25 - Have you read the NIST publication, "Protecting Controlled Unclassified Information in Non-federal Information Systems and Organizations" (NIST SP 800-171)?

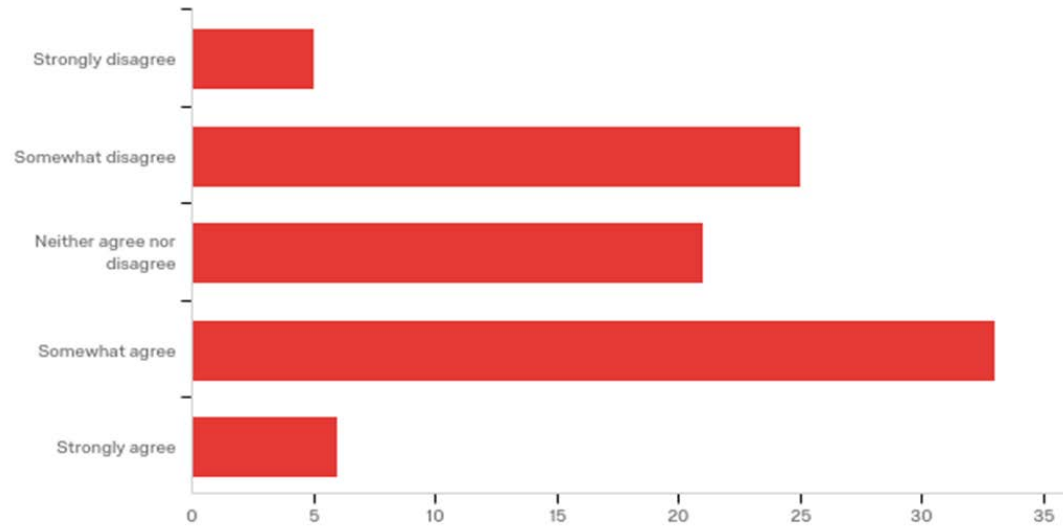


Q27 - Have you read the new DFARS regulation covering cyber security for controlled defense information (DFARS 252.204.7012)?

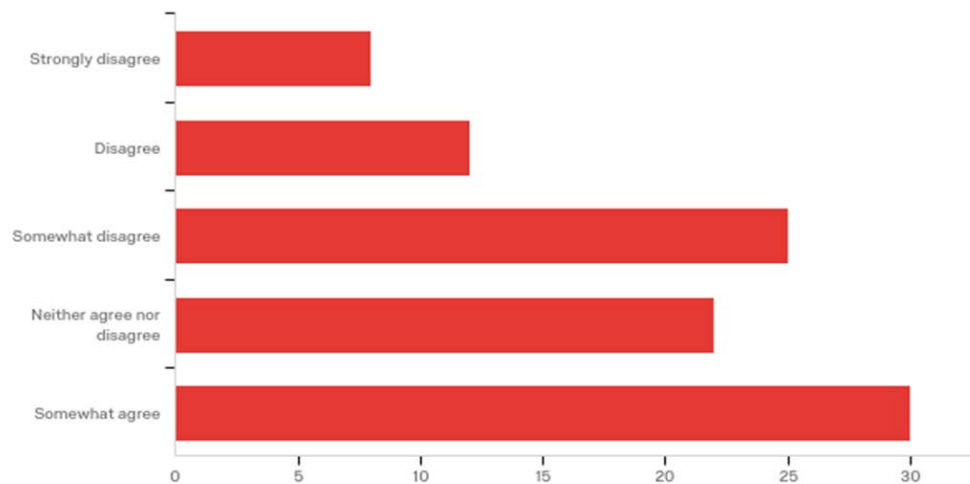


And...This Isn't Easy!

Q26 - The NIST publication SP 800-171 is clear and easy to understand?

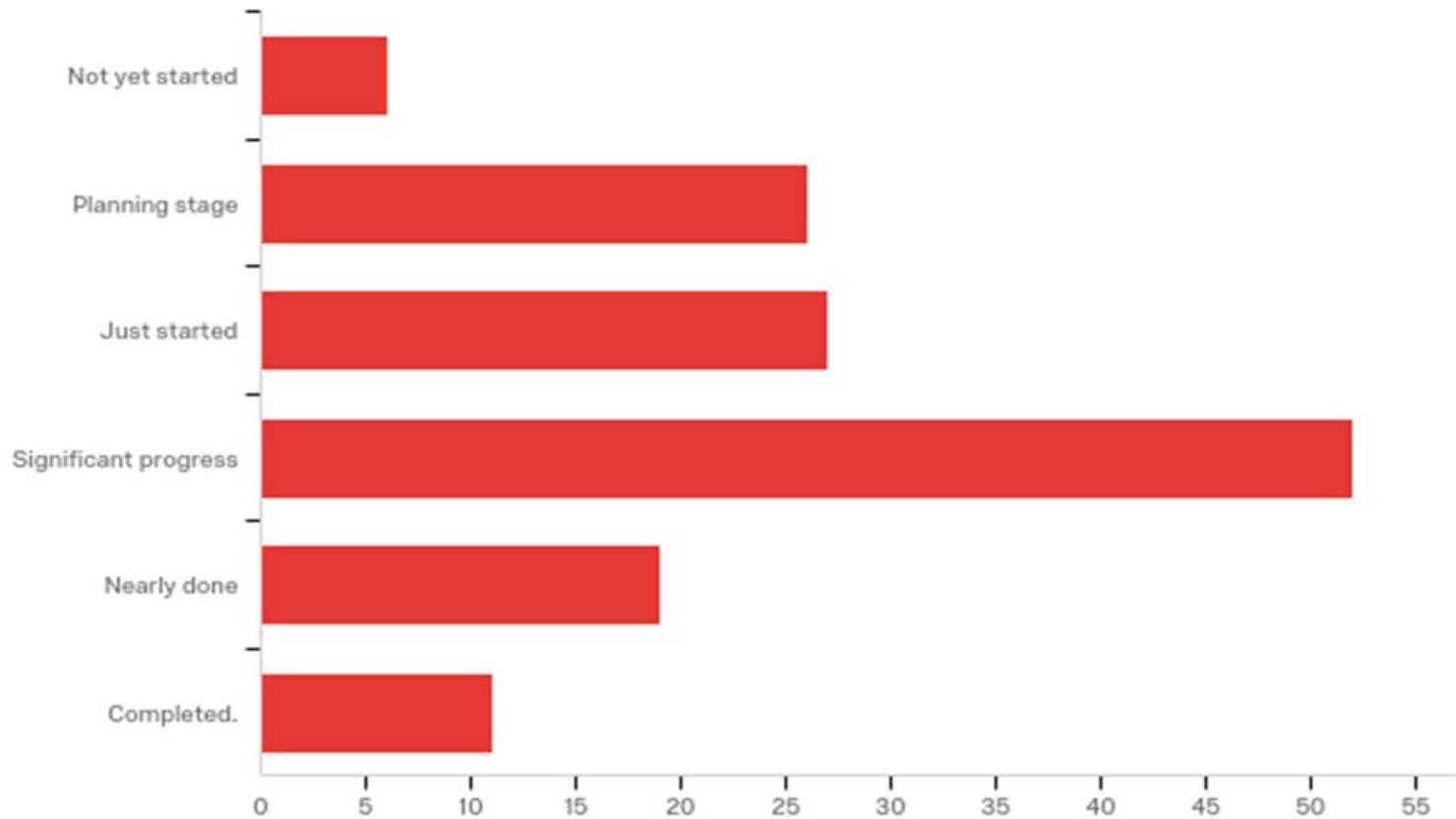


Q28 - The new DFARS 252.204.7012 regulation is clear and easy to understand.



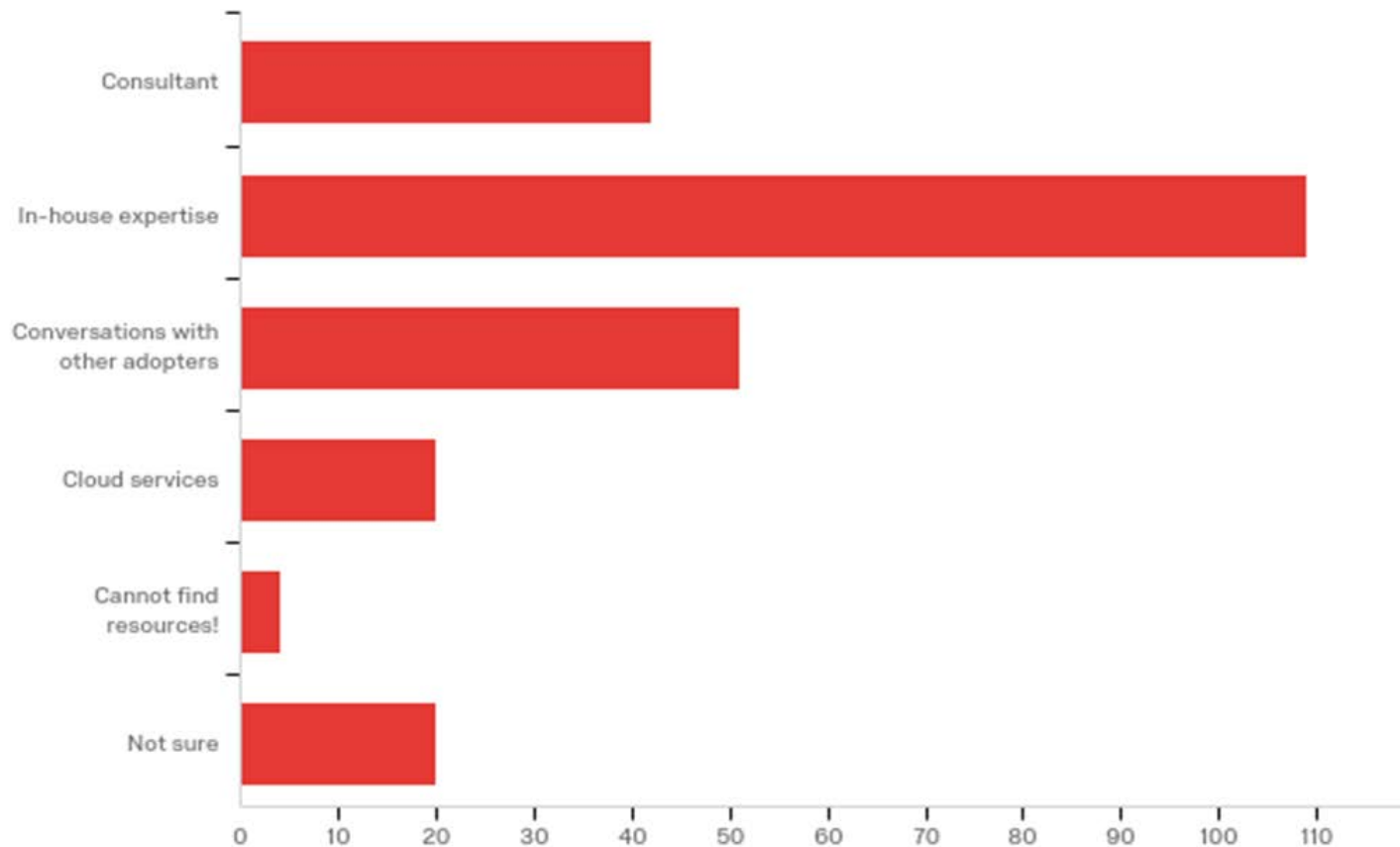
But Efforts Are Being Made – 1

Q10 - How far along is your organization in implementing the measures to comply with the new DFARS cyber security requirements? (pick one of the options provided below)



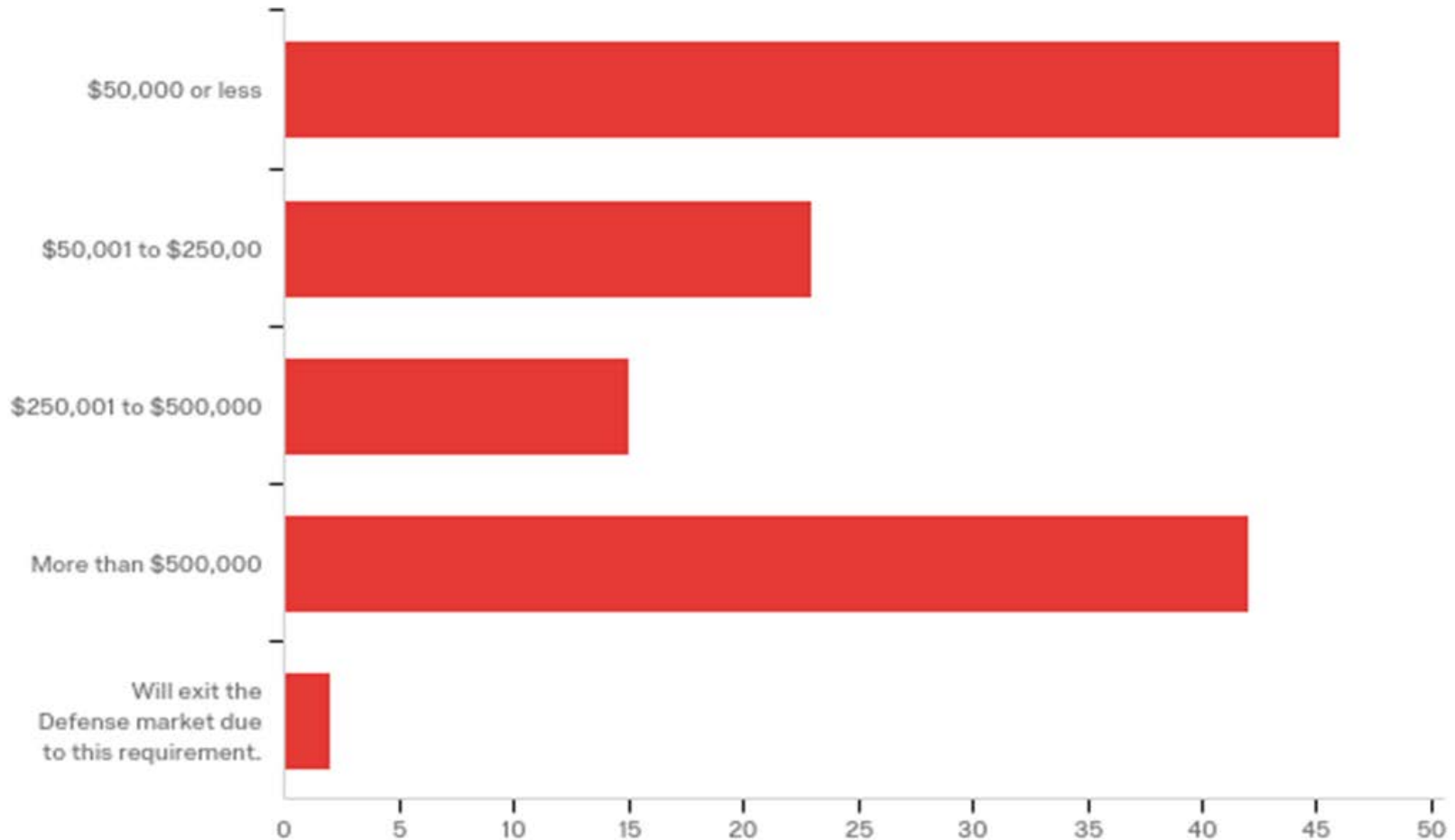
But Efforts Are Being Made – 2

Q11 - What resources have you used or are you planning to use to comply with the new cyber security requirements? (select all that apply)



But Will It Be Enough?

Q12 - How much has your organization budgeted to be compliant with the new cyber security requirements? (Please select only one)



- **Location: Wide distribution**
- **Size: >50% have over 500 employees**
- **Roles: Primarily Primes and First Tier**
- **% Gov't Sales: Most over 50%; for 30, over 90%**
- **Tenure to Gov't: ~70% over 15 years**
- **Revenues: Widespread, Most over \$50M**

Next Steps

- **Complete statistical analysis – June**
- **Reports done in July**
- **Need to move forward with potential research grants.**



