INSTITUTE FOR DEFENSE ANALYSES

Defense Contractor Cyber Data Collection Effort - Insights

C. R. Bucher

SLIDES ONLY

NO SCRIPT PROVIDED

September 2019

IDA Document NS D-10926
Log: H 2019-000553

INSTITUTE FOR DEFENSE
ANALYSES 4850 Mark Center Drive
Alexandria, Virginia 22311-1882

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication

This work was conducted by the IDA Systems and Analyses Center under contract HQ0034-14-D-0001, Project AX-1-3100, "Technical Analysis for the Director, Developmental Test and Evaluation (D(DT&E))," for the AX / D,DT&E / Director, Developmental Test and Evaluation. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Approved for public release; distribution is unlimited.

Acknowledgements

The authors would like to thank IDA committee, Dr. Steve Warner (chair), Dr. Serena Chan, and Dr. Gregory N. Larsen for providing technical review of this effort.

For More Information

John S. Hong, Project Leader
jhong@ida.org, 703-845-2564

Steve Warner, Director, SED
swarner@ida.org, 703-845-2096

Rigorous Analysis | Trusted Expertise | Service to the Nation

INSTITUTE FOR DEFENSE ANALYSES

IDA Document NS D-10926

Defense Contractor Cyber Data Collection Effort - Insights

C. R. Bucher

Summary

In support of task AX-1-310047 for Director, Developmental Test and Evaluation (D(DT&E)), the Institute for Defense Analyses (IDA) conducted a defense contractor outreach effort to understand, from a high-level perspective, how defense contractors incorporate cybersecurity into design and testing of defense programs, and to understand how D(DT&E) can better support contractor developmental cybersecurity testing. Nine defense contractors were initially contacted, and three responded for interviews. Five main insight areas emerged from the interviews: 1) cybersecurity as Risk Management Framework (RMF) and compliance versus cybersecurity as an engineering design-based approach, 2) improving requirements and contracts for contractor cybersecurity testing, 3) usefulness of cybersecurity table tops (CTTs), 4) shifting left with government test and evaluation (T&E) to contractor testing (CT) and the requirements needed for such a shift, and 5) lack of awareness by defense contractors of the six phases of the Department of Defense Cybersecurity T&E Guidebook. Potential actions for D(DT&E) to address these findings are presented.

(This page is intentionally blank)

Contents

(This page is intentionally blank)

1. Slides

(This page is intentionally blank)

IDA

Defense Contractor Cyber Data Collection Effort - Insights

Dr. Christine Bucher

1 October 2019

IDA | Background

Objective:

To understand, from a high-level perspective, how cybersecurity is incorporated into design and testing with defense contractors, and how the government, specifically Director, Developmental Test and Evaluation (D(DT&E)), can better support contractor developmental cyber testing efforts.

Approach:

- Created list of questions to understand defense contractor cybersecurity testing.
- Interviewed defense contractors (nine initially contacted, three responded).
- Summarized findings.
- Provided recommendations.

IDA | Main Insight Areas from Interviews

Five main areas emerged from defense contractor interviews:

1) Risk Management Framework (RMF) and Compliance
2) Contracts and Requirements
3) Cyber Table Tops (CTTs)
4) Shift Left with Test and Evaluation (T&E) to Contractor Testing (CT)
5) Six Phases of Department of Defense (DoD) T&E

1) RMF and Compliance

- Current cybersecurity testing is RMF and compliance.
- Need to move away from cybersecurity as just information assurance (compliance) to an engineering design approach – ***Services are not funding programs to do design-based cyber testing.***
- Contractors are recognizing the need for a cyber design approach and are taking some initiatives:
  - Lockheed Martin is doing exploratory testing (not compliance) to see where vulnerabilities exist.
  - Northrop Grumman stood up an internal Adversarial Assessment team in 2016, although not in any statement of work, indicating that Northrop Grumman has been doing risk reduction.

IDA | IDA Insights – Cont.

2) Contracts

- Any kind of cybersecurity testing that gets done comes down to contracts and ***requirements in the contract.***
  - ***If it is not specified in the contract, it does not get done!***
- Contractors bid to government requirements, which determine the level of cybersecurity that contractors ensure.
  - Requirements are currently based on RMF and compliance.
  - Penetration tests are the kind of requirements-driven tests contractors can do.
  - Adversarial Assessments are not something they can spec to and bid on.
  - Contractors know that coming government Developmental Testing/Operational Testing (DT/OT) cyber testing will be ultimately focused on mission effects, but since contractors test according to requirements in the contract, contractors will end up failing mission test.
    - Need to understand how to specify requirements better in contracts.
    - Use requirements to run test cases that are more representative of government testing (DT/OT).

2) Contracts - Continued

- Issues often overlooked and not included in contracts:
  - Frequency of testing, e.g., for vulnerabilities.
  - Specifying that a penetration test must be done – contractor is only responsible for developing a penetration test plan and not conducting it and providing a report.
  - Funding to fix cyber issues – money is often not allocated in contracts to fix issues, which leaves potential system vulnerabilities.

3) Cyber Table Tops

- CTTs are very useful and broadly used.
- ***Not all programs can afford a full CTT.***

4) Shift Left with T&E to Contractor Testing

- Contractors support shifting left to CT.
- Requires ***partnership*** between contractor and government to address concerns:
  - Fears that government will want contractors to bear sole responsibility for cyber T&E – need funding partnership with government.
  - High level of trust on contractor part – because during early stages of development, problems will often be found; and contractors do not want government reports indicating their products are not good.
  - Need reassurance from government that it's safe to mention that systems might have vulnerabilities, especially during development, and that it's open to constructive conversations to assess risk – government needs to take leadership on this issue and say, "It's safe to discuss this, and I'm here to help."

4) Shift Left with T&E to Contractor Testing – Cont.

- ***Resources*** become an issue.
- Many programs do not have money, resources, or tools to support cyber T&E (e.g., who pays for duplicate systems for CT?).
  - Northrop Grumman has internal resources for cyber testing:
    - Anechoic chambers
    - Hardware-in-the-loop labs
  - Lockheed Martin has invested money into cyber efforts:
    - Cyber Resiliency Levels (CRL) and Cyber Resiliency Systems Engineering (CRSE)
    - Avionics Cyber Range
    - Penetration Center of Excellence
    - Fuzzing tools and labs (Missiles and Fire Controls)
  - Government could do more to bear the cost for resources and tools.
    - Test and Evaluation Master Plan (TEMP) could provide resources for duplicate hardware, Systems Integration Laboratory, cyber ranges, Red Teams, senior engineers to work program, etc.

4) Shift Left with T&E to Contractor Testing – Cont.

- Contractors need to be provided ***intelligence and threat data*** to know what to test to, especially if doing design-based cyber testing – this needs to be an end-to-end process starting with threats.
  - Also, contractors need clearances for threat data and access to data (SIPRNet).

5) Six Phases of DoD Cyber T&E

- RMF understood very well – but the government does a poor job educating contractors on the six phases of DoD T&E.
- ***Few contractors are aware that DoD Cybersecurity T&E Guidebook exists***, or they don't understand role of T&E.

IDA | Summary of Findings and Potential Actions

- ***Finding:*** Services are not funding programs to do design-based cyber testing.
  Potential Action(s): Meet with OUSD(R&E) to inform them of findings and develop strategy for funding design-based cyber testing. To develop an adequate strategy, it will be necessary to engage the mission requirements writers, acquisition contracting community, chief information officer/chief information security officer, DoD Cost Assessment and Program Evaluation, sustainment community, services, and in the intelligence community in order to realistically design, build, and test that assures cybersecurity risks are addressed or able to be addressed.

- ***Finding:*** Requirements in contracts are critical in determining what extent of cyber testing is conducted.
  Potential Action(s):
  - Conduct industry round table discussion to understand how government can specify better requirements.
  - Mount an effort to ensure model contract language for generally acceptable practices, and to tailor contract language for specific needs.

IDA | Summary of Findings and Potential Actions (cont.)

- ***Finding:*** Shifting left with T&E to contractor testing requires the following:
  - Trusting partnership between contractor and government to address concerns
  - Support for resources from government
  - Accessibility to intelligence and threat data

Potential Action(s):

- Conduct industry round table discussion on shifting left with T&E to contractor testing and addressing the requirements and concerns for such testing.
- D(DT&E) should push to make sure contractor-led CTT and penetration testing are requirements in the TEMP for major defense acquisition programs. The TEMP should require the contractor cyber team to be engaged with the government adversarial team, and vice versa the government adversarial team aware of contractor testing.
- Engage industry through their Independent Research and Development programs to instrument their acquisition developments to produce the evidence that design-based cyber testing is finding and address both adversary access opportunities and vulnerability exposure weaknesses.

IDA | Summary of Findings and Potential Actions (cont.)

- ***Finding:*** Not all programs can afford a full CTT.

  Potential Action(s): Update the CTT Guidebook to provide tailored versions of the CTT process (like a mid-point CTT and a full-up CTT), and the difference in output between the different versions to know the results expected from each.

- ***Finding:*** Few contractors aware that T&E Guidebook exists, or they don't understand the role of DoD T&E.

  Potential Action(s):

  • Conduct educational campaign addressed to defense contractors about the six phases in DoD T&E Guidebook.

  • D(DT&E) should publish a guidance document that describes the minimum criteria for contractor-based testing to satisfy D(DT&E) cyber assessment requirements.

IDA

Backup

IDA | Defense Industry Outreach Data Collection Questions

1) How is cybersecurity test and evaluation incorporated into the development of products/systems?
2) Is cybersecurity testing only through contract, or is it done independently during development?
3) How often is cybersecurity testing conducted?
4) How do you scope what gets tested?
5) Do you have a standard process or playbook for cybersecurity testing? If so, is it tailored per product/system, or standard throughout company?
6) What kind of cybersecurity testing is performed (i.e., vulnerability scans, adversarial, etc.)?
7) Is resiliency worked into cybersecurity testing?

IDA | Defense Industry Outreach Data Collection Questions – cont.

8) Who conducts the testing? Do you have Red and Blue Teams? Is any preparation or coordination involved?

9) What kind of tools are used for cyber testing?

10) What kind of test environment do you test in?

11) What do you do with the results from testing?

12) Do you have limitations (technical, infrastructure) to testing?

13) Do you have any best practices for incorporating cybersecurity testing during development of product/system?

14) What do you think of "shifting left" with test and evaluation so that more of it occurs during contractor testing? What would be required for that?

Defense Industry Outreach Data Collection Questions – cont.

15) What can the Department of Defense do to better support contractor test and evaluation?

16) Do you have any other suggestions or recommendations?

Appendix A. Acronyms and Abbreviations

CRL	Cyber Resiliency Levels
CRSE	Cyber Resiliency Systems Engineering
CT	Contractor Testing
CTT	Cyber Table Top
D(DT&E)	Director, Developmental Test and Evaluation
DoD	Department of Defense
DT	Developmental Testing
IDA	Institute for Defense Analyses
OT	Operational Testing
OUSD(R&E)	Office of the Undersecretary of Defense, Research and Engineering
RMF	Risk Management Framework
SIPRNet	Secret Internet Protocol Router Network
T&E	Test and Evaluation
TEMP	Test and Evaluation Master Plan

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
10-2019

2. REPORT TYPE
IDA Publication

3. DATES COVERED *(From - To)*

4. TITLE ANDSUBTITLE

Defense Contractor Cyber Data Collection Effort - Insights

5a. CONTRACT NUMBER
HQ0034-14-D-0001

5b. GRANT NUMBER
____ ____ ____

5c. PROGRAM ELEMENT NUMBER
____ ____ ____

6. AUTHOR(S)

Christine R. Bucher (SED);

5d. PROJECT NUMBER
AX-1-3100

5e. TASK NUMBER
____ ____ ____

5f. WORK UNIT NUMBER
____ ____ ____

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

8. PERFORMING ORGANIZATION REPORT NUMBER

10926
H 2019-000553

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER
____ ____ ____

12. DISTRIBUTION / AVAILABILITY STATEMENT

13. SUPPLEMENTARY NOTES
____ ____ ____

14. ABSTRACT

The document summarizes a defense contractor outreach effort to understand, from a high-level perspective, how defense contractors incorporate cybersecurity into design and testing of defense programs, and to understand how the sponsor, Director, Development Test and Evaluation (D(DT&E)), can better support contractor developmental cybersecurity testing. Findings and potential actions for D(DT&E) are presented.

15. SUBJECT TERMS
Cybersecurity, defense contractor, developmental test and evaluation

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			John Hong (SED)
Unclassified	Unclassified	Unclassified	Unlimited		**19b. TELEPHONE NUMBER** *(include area code)* (703) 845-2564

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI std. Z39.18