January 2019

THE PATH TO A STRONGER DOD

A SUMMARY OF RECENT DEFENSE AUDITS

Authored By:

Drew Spaniel, Lead Researcher, ICIT
Parham Eftekhari, Executive Director, ICIT

ICIT Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

The Path to a Stronger DoD

A Summary of Recent Defense Audits

January 2019

Support ICIT

This publication and virtually all ICIT content is made freely available thanks to the generous support of our members who hail from critical infrastructure sector organizations and technology leaders from across our Nation.

Through objective research, publications, and educational initiatives, ICIT is cultivating a global cybersecurity renaissance by arming public and private sector leaders with the raw, unfiltered insights needed to defend our nation from digital threats.

Financial capital from generous donors is the lifeblood of the Institute and a force multiplier to our efforts. With your support, ICIT can continue to empower stakeholders with bleeding-edge research and actionable education that will improve the resiliency of our critical infrastructures, defend our democratic institutions, and empower generations of cyber leaders.

Please consider joining our community and becoming a part of this important movement. Together, we can hyper-evolve America's cyber posture.

Click Here to Learn More: https://icitech.org/support-icit/

Contents

Introduction: Knowledge is Power

In October 2018, hackers breached approximately thirty systems related to the defense acquisitions systems of the South Korean government. It is believed that the stolen documents contain information about arms procurement for the country's next-generation fighter aircraft and other sensitive military systems. Based on recent internal audits and reporting from the Government Accountability Office and Inspector General's office, the United States Department of Defense (DoD) may be susceptible to similar attacks in which sophisticated nation-state sponsored advanced persistent threats and cyber mercenaries could exfiltrate highly classified defense documents, steal intellectual property, plant malware on systems critical to national security, digitally neutralize defensive capabilities, or wholly seize control of weapons systems.

In this report, ICIT has summarized four of these recent audits and offers high-level recommendations members of the DoD community may consider to remediate the weaknesses and mitigate potentially devastating cyberattacks.

The first step in comprehensive cybersecurity and cyber-hygiene is identifying potential problems. While audits have unfortunately become an opportunity to criticize an organization for its weaknesses and failures, ICIT does not believe that this is a healthy or productive use of these assessments, and that this trend may result in the recommendations and insights found in these assessments to be overshadowed or overlooked. ICIT views audits as valuable tools which acknowledge gaps that exist and identify specific targets for investments and action.

Knowledge is power. While recent audits have identified a staggering number of vulnerabilities in DoD systems, we applaud the women and men of the DoD's cybersecurity, national security, and risk management teams for considering the feedback of these and other audits as they work tirelessly to defend some of our Nation's most critical assets from sophisticated nation state and cyber mercenaries. Our hope is that every public and private sector organization views audits not as threats, but as opportunities to improve and become more resilient against today's hyper evolving threat landscape.

Audit 1: Financial & Business Management Systems

A $1 Billion Audit Revealed Significant Cybersecurity Woes

A $1 Billion year-long audit of the Department of Defense, which began in December 2017, prompted approximately $560 million in remediation and system fixes corresponding to issues with inventory accuracy, cybersecurity discipline, and cyber-hygiene. Often unnoted is the fact that while the audit itself cost $413 million; the Pentagon spent an additional $406 million on audit remediation and $153 million on financial system fixes, for which it should be applauded.

The 236 page report details the findings of about 1,200 auditors from nine independent public accounting firms and staffers from the department's Office of the Inspector General who conducted 900 site visits at more than 600 department locations, including military bases, warehouses and depots. To give you a feel for the scope and scale of the audit, consider these statistics:

- The evaluation analyzed 55 percent of the department's $2.7 trillion in assets and $2.6 trillion in liabilities.
- Findings related to information technology security accounted for more than half of the more than 2,000 notices of findings and recommendations issued by the auditors [1] [2].
- Twenty-one separate component-level audits fed into the department-wide version.
- Examiners issued 1,119 separate notices of findings and recommendations (NFRs) related to IT.
- Among the military services and agencies, the Department of the Navy had 298 separate findings, including 52 that had already been identified in partial DoD audits in prior years, the Air Force had a total of 169 NFRs in the IT category, and the Army had 157 [2].

In the report summary, auditors found the department's "financial and business management systems and processes do not provide reliable, timely, nor accurate information." It also found "systemic shortfalls in implementing cybersecurity measures to guard the data protection environment" and "issues exist in policy compliance with cybersecurity measures, oversight, and accountability" [1].

One reason attributed to the adverse results is the incomplete implementation of the DOD's ERP system. According to the GAO, "ERP implementation has been delayed because of deficiencies in functional capability and the need for remedial corrective actions" GAO reported, "The DoD components will need to identify effective work-around processes or modifications to legacy systems that will enable audit readiness. Without fully deployed ERPs, the department will be challenged to produce reliable financial data and auditable financial statements without resorting to labor-intensive efforts, such as data calls or manual workarounds, or to provide reliable financial data on a recurring basis."

The DOD's more than 400 accounting-related IT systems were placed at the top of the list of 20 identified material weaknesses. The report states, "For example, to process and record contract payments, the [military] services depend on over a dozen IT systems that are owned and operated by other DoD components. Ineffective IT system controls can also result in significant risk to DoD operations and assets. For example, payments and collections could be lost, stolen, or duplicated as a result of weak IT controls. In addition, critical operations, such as those supporting national defense and emergency services, could be disrupted through weak IT controls." The IG reported that DOD organizations do not always follow regulations that require them to monitor the activities of privileged users and that that they are not consistently enforcing restrictions on what users can and can't do based on their specific roles. System access rights were not always revoked after users' left the organization and security controls meant to detect accidental or unauthorized changes to financial data were not always implemented. The IG recommends improving the internal controls for IT systems that process financial transactions because, "Improved internal controls on IT systems that process financial information will help the DOD both protect against and rapidly respond to cyber threats across different networks and systems" [3].

Following the audit, the IG flagged 800 shortcomings across the agency's IT systems and processes in 2018 in a January 2019 report. Much of the flawed tech is used to process contract payments and other transactions. Reportedly, the department failed to resolve more than 300 additional IT vulnerabilities that had been highlighted in prior years. The Navy was responsible for roughly 250 of the vulnerabilities and process flaws uncovered in the audit, while 96 were related to Air Force systems and another 64 were found in the Army's IT ecosystem. About 160 shortcomings were found in the department's enterprise-wide infrastructure [4]. The IG wrote, "Ineffective IT system controls can ... result in significant risk to DoD operations and assets. Payments and collections could be lost, stolen or duplicated as a result of weak IT controls. In addition, critical operations, such as those supporting national defense and emergency services, could be disrupted through weak IT controls."

Recommendations

Based on the findings of this audit, the DoD may consider the following actions:

- Secure financial and other ancillary IT systems that could be leveraged for adversarial lateral compromise of sensitive systems.
- Institute strong identity management and access controls across all systems
- Phase out legacy infrastructure in favor of more secure and efficient modern alternatives

Audit 2: Weapons Systems

US Weapons Systems May Be Vulnerable to Foreign Compromise

In October 2018, the US Government Accountability Office released a report to the US Senate Committee on Armed Services, entitled "Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities" which concluded that almost all weapons that were tested by the DOD between 2012 and 2017 had "mission critical" cyber vulnerabilities. The report explained that, "Using relatively simple tools and techniques, testers were able to take control of systems and largely operate undetected, due in part to basic issues such as poor password management and unencrypted communications." The GAO found that the DOD had an entire generation of systems that were built without incorporating cybersecurity throughout their development lifecycle. The results of the report were based on penetration tests the DOD itself undertook, as well as interviews with officials at various DOD offices [5] [6].

Poor cyber hygiene can be significantly detrimental to any network and the DOD testers discovered that some of the significant vulnerabilities discovered in the department's weapons systems began with poor basic credential security or lack of encryption. One tester was able to guess an admin password on a weapons system in nine seconds. Another tester managed to partially shut down a weapons system by employing the basic technique of scanning it. Default passwords were used on other weapons systems that used commercial or open source software because administers failed to change the default credentials. In some cases, testers were able to take full control of weapons systems. According to the report, “In one case, it took a two-person test team just one hour to gain initial access to a weapon system and one day to gain full control of the system they were testing.” DOD system administrators were often unable to detect the presence of a compromise. In one case, testers were in the weapons system for weeks but the administrators never found them despite the testers being intentionally “noisy.” Further, the report notes that when automated systems detected the testers’ intrusions, the humans monitoring the systems failed to understand what the intrusion detection technology was communicating [5] [6].

Worryingly, it appears that some at the DOD dismiss the findings of the report as unrealistic due to the access granted to the testers. The GAO stated, “In operational testing, DOD routinely found mission-critical cyber vulnerabilities in systems that were under development, yet program officials GAO met with believed their systems were secure and discounted some test results as unrealistic.” These DOD officials failed to recognize that adversaries, especially sophisticated APTs, are not constrained by the time constraints, limited funding, or restrictions placed on testers. The modest access initially granted to the testers pales in comparison to the capabilities of many cyber threats. When the DOD dismissed the results, they were dismissing the testing done by their own department since GAO audited assessments from DOD testers rather than conduct the tests itself. The testers, who were limited on time and resources, leveraged the most expedient and effective vulnerabilities to compromise each system. They did not identify or discover every vulnerability that an adversary could exploit and not all weapons were tested. The tests did not even evaluate industrial control systems, air-gapped systems, or counterfeit components. The report cautions that “Many program officials we met with indicated that their systems were secure, including some with programs that had not had a cybersecurity assessment.” Consequently, the GAO predicts that the DOD is only aware of a fraction of the vulnerabilities in their systems. The GAO found that only one out of twenty cyber vulnerabilities that the DOD had been alerted to in previous risk assessments had been fixed during the time period of the new report [5] [6].

GAO officials highlighted that hackers cannot yet take control over current weapons systems and turn them against the US because all tests were performed on computerized weapons systems that are still under development. The report cautions that "Nearly every conceivable component in DOD is networked. Weapon systems connect to DOD's extensive set of networks--called the DOD Information Network--and sometimes to external networks, such as those of defense contractors. Technology systems, logistics, personnel, and other business-related systems sometimes connect to the same networks as weapon systems. Furthermore, some weapon systems may not connect directly to a network, but connect to other systems, such as electrical systems, that may connect directly to the public Internet." One reason that these new computerized weapons systems are so vulnerable to cyber compromise is that until recently, the DOD did not prioritize "cyber" as part of the development process; however, it has begun to grasp the magnitude of the problem and taken a way of action. It instituted more comprehensive testing procedures and it made “cyber” a focus of its acquisition process.

Recommendations

Based on the findings of this audit, the DoD may consider the following actions:

- Implement Deliver Uncompromised and Security-by-Design methodologies
- Regularly audit and penetration test all system and components
- Institute greater credential management and access control policies and controls

Audit 3: Implementation of NIST Cybersecurity Framework

226 Cyber Recommendations To Go…Following a FY2018 cybersecurity audit of Department of Defense systems and their compliance with the NIST Cybersecurity framework, it was determined that the Pentagon has not implemented 266 cybersecurity-relevant recommendations. A January 9, 2019 Inspector General summary report of Department of Defense Cybersecurity from July 1, 2017 through June 30, 2018, found that “DoD Components implemented many of the agreed-upon corrective actions necessary to improve system weaknesses” however, the department “still faces challenges in managing cybersecurity risk to its network”. The audit conclusions include the results obtained from the analysis of four classified reports, and twenty unclassified reports that were issued between July 1, 2017, and June 30, 2018, by the Government Accountability Office and DoD's oversight community.

The report explains that, "Open recommendations can be either resolved or unresolved. Resolved recommendations are those that DoD management has agreed to implement but has not yet completed agreed-upon actions. Unresolved recommendations are those that DoD management disagrees with or provides alternative corrective actions for." While some of the open recommendations date back as far as 2008, the vast majority (151) originated in 2018, with the bulk of the remainder issued between 2012 and 2017. At the time of the January publication, it was reported that 112 of the 2018 recommendations were resolved according to the IG. This means that military managers have “agreed to implement” the recommendations but have not yet completed them. Alternately, 39 unresolved recommendations solicited disagreement or suggestions of “alternative corrective actions” from management [7] [8].

IT Governance Is a Major Struggle

The report identified the DOD’s greatest struggle as IT governance, stating, “Without proper governance, the DoD cannot assure that it effectively identifies and manages cybersecurity risk as it continues to face a growing variety of cyber threats from adversaries such as offensive cyberspace operations used to disrupt, degrade, or destroy targeted information systems,” the Pentagon IG writes. “The DoD must ensure that cybersecurity risks are effectively managed to safeguard its reliance on cyberspace to support its operations and implement proper controls and processes where weaknesses are identified to improve cybersecurity for the DoD.” The Department of Defense still has to address a multitude of cybersecurity gaps in "governance, asset management, information protection processes and procedures, identity management and access control, security continuous monitoring, detection processes, and communications” [7] [8]. Moreover, The Defense Contract Management Agency failed to ensure cyber specialists were properly trained and received necessary certifications; the Defense Health Agency and Army also failed to consistently secure systems that house electronic health data; and the Air Force also could not account for the various digital devices connected to its networks, and its branch leaders failed to guarantee cybersecurity was built into the design of various weapons systems.

Software Application Rationalization is Lacking Across the DoD

Software Rationalization - – the methodology implemented to identify whether existing applications are necessary, duplicative, or obsolete – is an important step for organizations to build into their acquisition process. The audit found that multiple branches of the military failed to rationalize their software applications because the Pentagon did not formalize a process to do so. According to the Department of Defense Inspector General, the Navy, Marine Corps and Air Force do not have consistent processes in place for software rationalization.

It should be noted that the Marine Corps and Navy have processes in place to prevent the purchase of duplicative software, although it is unknown how consistently the processes are being used. The U.S. Fleet Forces Command has a process to identify duplicate software applications after they were purchased; however, the process did not consider whether the software applications were installed or used on the network. The IG found that none of the commands has a comprehensive inventory of the applications operating on their networks. The Army was evaluated because its own Army Audit Agency conducted a similar review in 2017. The DOD CIO is required by the Federal IT Acquisitions Reform Act to provide an enterprise-wide plan for software rationalization [9].

Recommendations:

Based on the findings of this audit, the DoD may consider the following actions:

- Institute Identity Management Control and Governance
- Develop an enterprise-wide process for software application rationalization
- Establish guidance for DOD components commands to conduct periodic reviews and validate the accuracy of their software inventories
- Require the DOD CIO’s office to validate that components are eliminating any duplicate or obsolete software

Audit 4: Ballistic Missile Defense System Facilities

Ballistic Missile Defense System Defense is Woefully Vulnerable

On December 10, 2018, the Department of Defense Inspector General publically released the results of an audit of the security controls and processes at DoD facilities to protect ballistic missile defense system (BMDS) technical information on classified networks from insider and external cyber threats, concluding that "the Army, Navy, and MDA did not protect networks and systems that process, store, and transmit BMDS technical information.” The audit was conducted “in response to a congressional requirement to audit the controls in place to protect BMDS technical information, whether managed by cleared Defense contractors, or by the Government. Cleared contractors are entities granted clearance by the DoD to access, obtain, or store classified information, to bid on contracts, or conduct activities in support of DoD programs." Only classified networks were analyzed since classified and unclassified BMDS technical information is not stored, processed, or transmitted across unclassified networks. Additionally, an earlier report, released on March 29, 2018, on the effectiveness of logical and physical access controls in place to protect BMDS technical information at Missile Defense Agency (MDA) contractor locations identified systemic weaknesses at the contractor locations concerning network access, vulnerability management, and the review of system audit logs [10].

The Inspector General's report evaluated five randomly selected sites. Currently, the MDA has 104 ballistic missile locations and intends to build another 10 in the near future [3]. The audit determined that officials did not consistently protect BMDS technical information through the implementation of security controls and processes. Some of the findings of the evaluation include a severe lack of encryption, multifactor authentication mechanisms, and antimalware applications; unpatched vulnerabilities on systems, including some that are nearly 28-years old; and major physical security issues pertaining to access to server racks, removable media, and sensitive systems.

Poor Access Controls Could Enable Adversaries to Access Sensitive Networks and Systems

A lack of multifactor authentication was found to be the one of the largest weaknesses across the sample sites. When hired, MDA employees are allocated secure access credentials and a common access card (CAC) to access BMDS systems and networks. All new MDA workers must use multifactor authentication within two weeks of being hired; however, the DOD IG report states that at three of the five inspected locations many users did not employ multifactor authentication using CAC and sufficient governance was not in place to mandate the access control. At one site, the network was never configured to support multifactor authentication. In the absence of multifactor authentication, employees are vulnerable to phishing attacks or impersonation from remote attackers or insider threats [3].

Unpatched and Unprotected Systems Remain Vulnerable to Remote Compromise

IT administrators failed to apply security patches to computers and adjacent network systems at three of the five inspected sites. Consequently, adversaries could leverage the unpatched vulnerabilities (some going back as far as 1990) to compromise the systems. One location lacked intrusion detection and prevention systems. The report states, "Without intrusion detection and prevention capabilities, [REDACTED] cannot detect malicious attempts to access its networks and prevent cyberattacks designed to obtain unauthorized access and exfiltrate sensitive BMDS technical information from occurring."

Systems were also vulnerable due to a lack of policy related governance regarding access control and user privileges. All five of the inspected facilities failed to maintain a database of written justifications detailing why employees were permitted access to the BMDS network. Officials did not know why employees needed access to the system, and could not enforce a least privilege access hierarchy. Furthermore, DOD IG investigators selected a small sample of employees from each location and requested their access forms. At each site, access forms were incomplete and in some instances, administrators could not provide any forms for some personnel [3].

Systems were Vulnerable to Insider Threats and Malicious Removable Media

Investigators discovered unlocked and easily accessible server racks at two locations. Further, at three locations, data was not required to be encrypted when transferred between air-gapped systems. As a result, any attacker or insider threat could have plugged in a removable media device loaded with malicious files or firmware and laterally infiltrated the network. The impact of a sophisticated malware, such as Black Energy, on these critical systems could prove devastating as a demonstration of geopolitical might or as a coordinated stage in multi-vector attack campaign. Malicious insider activity could have gone unnoticed because at several of the MDA bases, surveillance cameras failed to cover the entire base, creating gaps that an attacker could exploit to enter the groundwork and buildings. Additionally, some door sensors reported doors as shut when they were not and some facilities did not lock. MDA personnel did not challenge auditors who entered buildings without proper badges; thereby demonstrating that unauthorized personnel could infiltrate top secret buildings [3].

Recommendations

The audit of the “Security Controls at DoD Facilities for Protecting Ballistic Missile Defense System” included a robust set of recommendations compared to the other audits covered in this report. ICIT has included these recommendations and findings at length below.

The key findings of the audit were that Network administrators and data center managers did not [10]:

- Lock server racks
- Protect and monitor classified data stored on removable media
- Encrypt BMDS technical information during transmission
- Require the use of multifactor authentication to access BMDS technical information
- Implement intrusion detection capabilities on classified networks
- Identify and mitigate known vulnerabilities (at three of the five visited sites)
- Require written justification to elevate user privileges and system access

Further, security officers at the facilities did not consistently impose physical security controls to prevent unauthorized access to the facilities that managed BMDS technical information. The security control weaknesses existed because officials did not consistently verify the effectiveness of implemented controls or assess the impact of missing controls. The report concluded that, “Without well-defined, effectively implemented system security and physical access controls, the MDA and its business partners may disclose critical details that compromise the integrity, confidentiality, and availability of BMDS technical information. The disclosure of technical details could allow U.S. adversaries to circumvent BMDS capabilities, leaving the United States vulnerable to deadly missile attacks. Increasing threats of long-range missile attacks from adversaries requires the effective implementation of system security controls to help reduce the number of exploitable weaknesses that attackers could use to exfiltrate BMDS technical information" [10].

Across BMDS facilities it is recommended that [10]:

- Employ multifactor authentication
- Enforce the use of multifactor authentication to access systems that process, store, and transmit BMDS technical information or obtain a waiver from using multifactor authentication from the DoD Chief Information Officer
- Mitigate or remediate vulnerabilities in a timely manner
- Conduct regular audits and develop plans to identify, monitor, and remediate vulnerabilities
- Encrypt BMDS technical information stored on removable media
- Restrict the access of removable media
- Implement intrusion detection capabilities
- Evaluate lapses in physical security and install cameras and other technical controls to monitor individuals' activities throughout sensitive facilities.

Additionally, the report recommends that the Chief Information Officer should [10]:

- Enforce the use of multifactor authentication to access systems that process, store, and transmit BMDS technical information or obtain a waiver from using multifactor authentication
- Mandate the implementation of intrusion detection capabilities on networks that maintain BMDS technical information
- Develop and implement procedures to secure server racks and control server rack keys
- Maintain access request forms that include written justification to support the need for access to networks and systems that contain BMDS technical information.
- Encrypt BMDS technical information stored on removable media
- Develop and implement a process to identify individuals who are authorized to use removable media as well as procedures to monitor the type and volume of data transferred to and from removable media
- Establish policies, procedures, guidelines, and technical and nontechnical controls pertaining to personnel and other individuals with access to systems and facilities.

Conclusion

Over the years, audits have gained a reputation as an opportunity to criticize an organization for its weaknesses and failures. ICIT does not believe that this is a healthy or productive use of these assessments, and that this trend may result in the recommendations and insights found in these assessments to be overshadowed or overlooked. Audits are an invaluable tool for identifying potential shortcomings, problems, and lapses in security. While it is difficult for any organization to receive constructive criticism, and easy for those on the outside to point the finger, it is a necessary part of improvement. Peers must support organizations as they digest audit feedback and work to grow and learn from these assessments.

Four audits of United States defense systems have found hundreds of vulnerabilities and weaknesses in critical weapons systems and supporting networks. If an adversary were to exploit the identified vulnerabilities, they could exfiltrate sensitive data, render vital systems inoperative, or seize control of American weapons systems. The high-level recommendations detailed throughout this publication were based on the outstanding work of the DoD's audit teams and they can be used to mitigate the threat of foreign compromise if acted upon in a timely manner.

ICIT is confident that the members of the Defense Industrial Base and DoD communities will work together to address these issues and continue to improve the resiliency of our nation's military.

Sources

[1] C. Kenney, "$1B Department of Defense Audit Stresses Cybersecurity Failings", Govtech.com, 2018. [Online]. Available: http://www.govtech.com/security/1B-Department-of-Defense-Audit-Stresses-Cybersecurity-Failings.html. [Accessed: 28- Jan- 2019].

[2] J. Serbu, "Nearly half of Pentagon's audit failures can be chalked up to bad IT", *Federal News Network*, 2019. [Online]. Available: https://federalnewsnetwork.com/defense-main/2019/01/nearly-half-of-pentagons-audit-failures-can-be-chalked-up-to-bad-it/. [Accessed: 28- Jan- 2019].

[3] C. Cimpanu, "US ballistic missile systems have very poor cyber-security | ZDNet", ZDNet, 2018. [Online]. Available: https://www.zdnet.com/article/us-ballistic-missile-systems-have-very-poor-cyber-security/. [Accessed: 28- Jan- 2019].

[4] "Understanding the Results of the Audit of the DoD FY 2018 Financial Statements | Oversight.gov", Oversight.gov, 2018. [Online]. Available: https://oversight.gov/report/dod/understanding-results-audit-dod-fy-2018-financial-statements. [Accessed: 28- Jan- 2019].

[5] "WEAPON SYSTEMS CYBERSECURITY: DOD Just Beginning to Grapple with Scale of Vulnerabilities", Gao.gov, 2018. [Online]. Available: https://www.gao.gov/assets/700/694913.pdf. [Accessed: 28- Jan- 2019].

[6] E. Dreyfuss, "US Weapons Systems Are Easy Cyberattack Targets, New Report Finds", WIRED, 2018. [Online]. Available: https://www.wired.com/story/us-weapons-systems-easy-cyberattack-targets/. [Accessed: 28- Jan- 2019].

[7] "Summary of Reports Issued Regarding Department of Defense Cybersecurity From July 1, 2017, Through June 30, 2018", Media.defense.gov, 2018. [Online]. Available: https://media.defense.gov/2019/Jan/11/2002078551/-1/-1/1/DODIG-2019-044.PDF. [Accessed: 28- Jan- 2019].

[8] B. Mitchell, "Pentagon faces backlog of more than 260 cyber weaknesses, some a decade old - FedScoop", FedScoop, 2018. [Online]. Available: https://www.fedscoop.com/pentagon-cybersecurity-vulnerabilities-backlog/. [Accessed: 28- Jan- 2019].

[9] B. Mitchell, "Pentagon needs departmentwide software rationalization strategy, IG says - FedScoop", FedScoop, 2018. [Online]. Available: https://www.fedscoop.com/dod-software-rationalization-ig-report/. [Accessed: 28- Jan- 2019].

[10] "Security Controls at DoD Facilities for Protecting Ballistic Missile Defense System Technical Information DODIG-2019-034", Department of Defense Office of Inspector General, 2018. [Online]. Available: https://www.dodig.mil/reports.html/Article/1713611/security-controls-at-dod-facilities-for-protecting-ballistic-missile-defense-sy/. [Accessed: 28- Jan- 2019].