Recommendation 77: Require role-based planning to prevent unnecessary application of security clearance and investigation requirements to contracts.

Problem

DoD sometimes incorrectly applies security clearance and investigation requirements to unclassified contracts, reducing the talent pool from which contractor companies can recruit and exacerbating the substantial investigation backlog. The National Background Investigations Bureau (NBIB) backlog currently exceeds 657,000 personnel investigations and requires on average more than 200 days to complete a background investigation.[1] In many cases, these contract requirements violate the need-to-know principle that guides the National Industrial Security Program (NISP). In addition to reducing the talent pool from which contractor personnel can be recruited, unnecessary clearance requirements increase the investigation backlog and add administrative burden to both DoD and contractor companies.

Background

Unnecessary requirements for cleared personnel place a substantial burden on contractor companies and disincentivize hiring new, innovative employees. DoD has stated repeatedly its desire to attract talent from the commercial marketplace where the vast majority of innovation and technology development now takes place. The personnel who work in this marketplace generally do not have security clearances and many are not willing to subject themselves to either the inconvenience associated with the process or the protracted delay waiting for the results of an investigation and adjudication. It stands to reason that an individual with in-demand skills would prefer a more streamlined hiring process without such dependencies.

The NBIB backlog is a governmentwide problem, but 75 percent of government clearances are for DoD jobs. In 2005, GAO added the personnel security clearance process to its High Risk List—a list that "calls attention to the agencies and program areas that are high risk due to their vulnerabilities to fraud, waste, abuse, and mismanagement or are most in need of broad reform."[2] After demonstrating progress in 2011, the security clearance process was removed from the list, only to reappear in 2018. This recurrence was attributed to large growth in the clearance backlog, a previous security breach of the background investigation IT system, lack of a discernable plan to address the backlog, investigator capacity, or reform effort delays.[3] Although the report listed numerous factors, GAO did not evaluate whether DoD's 3.6 million clearance holders met the need-to-know requirement for having access to classified data. Defense Security Service (DSS) personnel estimate as many as 10 to 30 percent of contractor secret clearances are unnecessary.[4]

The government communicates contract clearance requirements through the DD Form 254, Department of Defense Contract Security Classification Specification, "for the protection of information in the

---

[1] Derek B. Johnson, *Security Clearance Backlog Drops 9 Percent,* FCW, September 25, 2018, accessed September 27, 2018, https://fcw.com/articles/2018/09/25/clearance-backlog-drops.aspx?m=1/.
[2] GAO, *Overview: High Risk List, GAO-17-317,* January 2018 edition, accessed October 31, 2018, https://www.gao.gov/highrisk/overview.
[3] GAO, *High Risk List, GAO-17-317,* January 2018 edition, accessed June 25, 2018, https://www.gao.gov/highrisk/govwide_security_clearance_process/why_did_study#t=1
[4] Defense Security Service, interview with Section 809 Panel Staff, June 13, 2018.

possession of cleared contractors associated with a classified contract."[5] To access material requiring confidential, secret, and top secret clearances, contractors must obtain a Facility Security Clearance (FCL) from DSS based on DD Form 254 requirements. The FCL is particularly important when common contract language contains requirements such as "[A]ll Contractor personnel performing on this TO shall possess or be eligible to obtain a SECRET security clearance" even on an unclassified system.[6] Unnecessary security requirements such as these make maintaining an FCL a necessity to compete on contracts. DSS conducts annual security reviews of cleared contractors to ensure safeguards are employed and National Industrial Security Program Operating Manual procedures are followed. These reviews include verifying a valid need to know exists, and DSS can rescind an FCL based on failure to demonstrate a need to know, regardless of the contract's DD Form 254. As a result, unnecessary classification leaves contractors vulnerable to termination of its FCL through no fault of their own. According to some at DSS who monitor and process contractor personnel security eligibility and access, contractors face "a losing battle in most circumstances…[they] do not want to fight their GCA/COR [Government Contracting Agency/Contracting Officer Representative] due to possible backlash."[7]

Once an FCL is approved and a classified contract awarded, the contractor uses the same systems as the government to manage cleared personnel. Considering the large clearance backlog and nearly 9-month average timeline for new investigations, contractors are incentivized to take the path of least resistance and settle for individuals with a current clearance, even if they are less qualified. The most qualified personnel languish waiting on clearances and ultimately move on to other opportunities. The real-world effect of the backlog on the industry talent pool was captured in a Senate intelligence hearing in March 2018:[8]

> *New careers are put on hold, top talent is lost to nondefense industries, and programs that will provide critical warfighter capabilities are delayed. And these impacts come with a real-world price tag, resulting in otherwise unnecessary increases in program costs and inefficient use of taxpayer dollars.*

The process levies unnecessary requirements on contractors and makes DoD unattractive to top talent.

Discussion

Most government contractors work on unclassified programs and do not require national security clearances.[9] This workforce consists of support contractors, such as acquisition support or cost analysis support, who will never access classified information and only require credentialing and access to an

[5] Defense Security Service, Public Affairs Office, *What is a DD Form 254?,* DSS Access Magazine, Volume 3, Issue 1, Spring 2014, 10, accessed June 20, 2018, http://www.dss.mil/documents/about/DSS_ACCESS_v3i1_Web.pdf.
[6] Excerpt from an Army Performance Work Statement (PWS) Small Business Task Order.
[7] Defense Security Service, interview with Section 809 Panel Staff, June 13, 2018.
[8] U.S. Senate Select Committee on Intelligence, Hearing Video, Mar. 7, 2018, accessed June 25, 2018, https://www.intelligence.senate.gov/hearings/open-hearing-security-clearance-reform.
[9] According to a 2014 report on security clearance determinations from the Director of National Intelligence, 483,185 contractor personnel were eligible for a Confidential or Secret clearance, whereas in 2015 a Volcker Alliance issue paper reported the total number of government contractor personnel ("contract employees") was 3,702,000. Office of the Director of National Intelligence, *2014 Security Clearance Determinations Report*, 4, accessed October 31, 2018, https://www.dni.gov/files/documents/2015-4-21%20Annual%20Report%20on%20Security%20Clearance%20Determinations.pdf. Paul C. Light, *The True Size of Government,* Issue Paper, The Volker Alliance, October 5, 2017, accessed October 31, 2018, https://www.volckeralliance.org/publications/true-size-government.

unclassified email system. There are already governmentwide and DoD-specific processes in place to complete this credentialing, in addition to the security clearance process. The 2008 Homeland Security Presidential Directive (HSPD) 12 established minimum standards for issuance of Personal Identity Verification (PIV) cards and Title 32 CFR established the IT security clearance standards. A PIV card and a Tier 1 investigation, formerly the National Agency Check with Inquiries (NACI), is the minimum standard for an individual to access federal facilities and unclassified systems such as DoD email.

HSPD-12 charged the Office of Personnel Management (OPM) to "ensure the effective, efficient and timely completion of investigations and adjudications relating to eligibility for logical and physical access." The PIV card is the first step to establish eligibility. Some of the criteria needed to grant a PIV card to individuals include the following:[10]

- The individual is not known to be or reasonably suspected of being a terrorist.
- The employer is able to verify the individual's claimed identity.
- There is no reasonable basis to believe the individual has submitted fraudulent information concerning his or her identity.
- There is no reasonable basis to believe the individual will attempt to gain unauthorized access to classified documents, information protected by the Privacy Act, information that is proprietary in nature, or other sensitive or protected information.
- There is no reasonable basis to believe the individual will use an identity credential outside the workplace unlawfully or inappropriately.
- There is no reasonable basis to believe the individual will use Federally-controlled information systems unlawfully, make unauthorized modifications to such systems, corrupt or destroy such systems.

HSPD-12 also standardized the NACI, now known as the Tier 1 investigation, for issuing an identity credential. It includes an NAC with "written inquiries to past employers, schools, references, and local law enforcement agencies covering the past five years and if applicable, of the appropriate agency for any identified arrests."[11] Tier 1 provides confidence an individual will not misuse information or seek to gain unauthorized access to classified data.

In addition to governmentwide credentialing, DoD also requires contractors with a valid need to know for accessing defense IT systems be categorized by the positions they fill. A 1978 change to Title 32 CFR introduced the three Automated Data Processing (ADP) position categories based on potential threats to IT systems. These criteria are used today via the DD Form 2875, System Authorization Access Request, for every DoD government employee, contractor, and Military Service member to document

[10] OPM Memorandum, *Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12,* July 31, 2008, accessed June 26, 2018, https://www.opm.gov/suitability/suitability-executive-agent/policy/final-credentialing-standards.pdf.
[11] "Security Clearance Investigations Process Updated," William Henderson, ClearanceJobs, October 9, 2011, accessed July 12, 2018, https://news.clearancejobs.com/2011/10/09/security-clearance-investigations-process-updated/.

their level of access in DoD IT systems. They also establish employees' responsibility and involvement in IT systems and the commensurate security clearance needed.[12]

- ADP–I positions: Critical-Sensitive Positions requiring a Tier 5 background investigation
  - Those positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain.
- ADP–II positions: Noncritical-Sensitive Positions requiring a Tier 3 background investigation
  - Those positions in which the incumbent is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority of the ADP–I category to insure the integrity of the system.
- ADP–III positions: Nonsensitive positions requiring a Tier 1 background investigation
  - All other positions involved in computer activities.

The HSPD-12 requirements for credentialing and the CFR IT ADP criteria ensure personnel are adequately screened and given the proper level of access to IT systems. Used in concert, these programs allow the government to confidently plan by individual role and limit overclassifying contracts.

Conclusions

Although NBIB plans a new National Background Investigation System to "address security concerns and provide a continuous vetting process to reduce errors and provide efficiencies," it will not change the process or reduce the number of unnecessary clearances.[13] For unclassified DoD contracts, the apparent fallback position of requiring all cleared personnel is a costly burden to the government and the contractor. Doing so incentivizes contractors to provide cleared but less qualified personnel due to the large increase in new clearance requests and reinvestigations. DoD loses the opportunity to hire quality personnel by settling for an expedient solution, and highly qualified applicants move to nondefense opportunities. Section 925 of the FY 2018 NDAA Conference Report states "The background investigation process is broken" and the current security clearance process causes a "degradation in workforce quality, as high-performing personnel with the best alternatives are unlikely to wait for many months to begin work for the U.S. Government."[14] One way to reduce the clearance burden on contractors is to scrutinize each clearance/investigation requested based on the role from the DD Form 2875.

[12] Defense Industrial Personnel Security Clearance Program, 32 C.F.R. 155.
[13] "DISA Modernizing Clearance Process with Continuous Monitoring," Lauren C. Williams, Defense Systems, June 22, 2018, accessed June 25, 2018, https://defensesystems.com/articles/2018/06/22/disa-clearance-nbis-tech.aspx?s=ds_250618,.
[14] FY 2018 NDAA, Conference Report to Accompany H.R. 2810, Report 115-404, November 9, 2017, 905, accessed October 16, 2018, https://www.congress.gov/115/crpt/hrpt404/CRPT-115hrpt404.pdf#page=943.

There are few clearances required for unclassified systems aside from those needed for elevated permissions that could compromise the system. The DD Form 254 should be the authoritative source for clearance requirements based on consolidated and detailed information from the OPM Position Designation Tool and employee DD Form 2875, which provides the job title, justification, clearance held, and ADP level designation for each role in the organization. Section 13 of the DD Form 254, Security Guidance, is the ideal consolidation point to communicate every role that requires a security clearance or a Tier 3 or Tier 5 investigation. Documents can be attached within Section 13 to clearly specify the contract security requirements. If properly planned and aligned with the DD Form 254, this role-based requirement could drastically reduce the number of clearance requests thereby providing improved access to uncleared talent.

Implementation

Legislative Branch

- There are no statutory changes required for this recommendation.

Executive Branch

- Develop policy to ensure clearance requirements in contracts are based only on valid security requirements that do not violate the NISP need-to-know principle.
- Issue guidance requiring role-based planning using the OPM Position Designation Tool to inform the DD Form 254, Department of Defense Contract Security Classification Specification.
- Expand use of the DD Form 254 to include use in unclassified contracts where Tier 3 and Tier 5 investigations are required based on ADP positions.
- Require use of DD Form 2875, System Authorization Access Request, to inform the DD Form 254 of required Tier 3 and Tier 5 investigations where no access to classified exists.
- Include personnel clearance planning in programs of instruction for DoD acquisition professionals and personnel generating contract investigation and clearance requirements.

Implications for Other Agencies

- Although there are no explicit cross-agency implications for this recommendation, other agencies could benefit from using role-based planning for security clearances.