Hearing Date: 6 March 2018
Committee: SSCI
Member: Senators Burr and Warner
Witness: ODNI/NCSC, Mr. Brian D.
Info Current as of: July 2, 2018

Question 1: Compliance & Enforcement.

Question 1a: Is the Security Executive Agent (SecEA) responsible for reviewing each government agency's compliance with laws, executive orders, and policies regarding the security clearance process? If yes, does this duty include reviewing the policies for reciprocity and/or the robustness of programs for continuous evaluation and insider threat?

Answer: Yes, the Security Executive Agent (SecEA), is responsible for conducting Executive Branch oversight of investigations and adjudications for personnel security clearances. This includes development and implementation of uniform and consistent policies and procedures; standardization of security questionnaires, financial disclosure requirements, polygraph policies and procedures, and reciprocal recognition of accesses to classified information. The SecEA is also the final authority for designating an authorized investigative or authorized adjudicative agency. This oversight includes the establishment of policies for continuous evaluation and insider threat programs, as well as monitoring compliance.

Question 1b: Which agency's processes does the SecEA review? How often is this review conducted?

Answer: In executing SecEA oversight responsibilities, on April 29, 2014, the DNI established the Security Executive Agent National Assessment Program (SNAP) to review department and agency (D/A) personnel security programs in the areas of security clearance initiation, investigation, adjudication, and application of due process. The annual review process assesses select D/A compliance with the policies and procedures governing the conduct of investigations and adjudications of eligibility for access to classified information or eligibility to hold a sensitive position government-wide. In addition, the ODNI regularly reports to Congress, via Congressionally Directed Actions on our processes and performance.

Question 1c: What assessments or reports does the SecEA issue to the agency or to Congress on such compliance?

Answer: The DNI has responded to Congressionally Directed Actions mandated in the 2010-2017 Intelligence Authorization Acts on numerous topics related to security clearance timeliness, backlog, reciprocity, and security clearance determinations for the Executive Branch. The following is a current list of these CDAs: Improving the Periodic Investigation Process, Security Clearance Determinations, Resolution of Backlog of Overdue Periodic Reinvestigations, Assessment of Timeliness of Future Periodic Reinvestigation, Insider Threat, and Continuous Vetting, Enhancing Government Personnel Security Programs - Implementation Plan.

Question 1d: What are the SecEA's means of enforcing compliance at a particular agency (e.g. through budgets, withholding certain certifications)?

Answer: The SecEA is given authority in Executive Order (E.O.) 13467, as amended, to designate an investigative or adjudicative agency. The SecEA may rescind a D/A's investigative or adjudicative authority if it is unable or unwilling to comply with applicable standards. The SecEA personally issues a letter to each agency head to inform them of their annual security program performance. If an agency does not meet performance goals, the agency head is required to submit a Corrective Action Plan with milestones and a

date of completion. The SecEA staff follows up with these organizations regularly until they achieve compliance and the desired end-state.

Hearing Date: 6 March 2018
Committee: SSCI
Member: Senators Burr and Warner
Witness: ODNI/NCSC, Mr. Brian D.
Info Current as of: July 2, 2018

Question 2: Trusted Workforce 2.0.

Question 2a: Who is involved in the DNI-led "Trusted Workforce 2.0" initiative? Are representatives from industry, think tanks, Government Accountability Office, or Congress involved?

Answer: The Trusted Workforce 2.0 initiative is led by the SecEA and Suitability Executive Agent (SuitEA) in concert with the other Performance Accountability Council (PAC) Principal Organizations, the Office of Management and Budget, the Office of the Undersecretary of Defense (Intelligence) and the National Background Investigations Bureau. Trusted Workforce 2.0, which began in March 2018, is supported by Executive Branch senior leadership, change agents, and innovative thinkers from government and industry.

Question 2b: What is the scope of the "Trusted Workforce 2.0" effort?

Answer: Trusted Workforce 2.0 is a fulsome, "clean slate" review of the vetting enterprise. The initiative will serve as the foundation for a trusted workforce while keeping pace with emerging technologies, capabilities, and opportunities to continuously identify, assess, and integrate key sources of information. Trusted Workforce 2.0 will chart a bold path forward for transforming the vetting enterprise in the areas of policy, governance, business processes and modernization of information technology architecture. This aggressive effort may require additional resources from Congress. We look forward to partnering with agency leadership and private industry to transform our vetting enterprise into a system that protects our nation's sensitive equities and meets the needs of the workforce.

Question 2c: Will the DNI initiative produce any recommendations or policy changes?

Answer: Yes. The intent of Trusted Workforce 2.0 is to identify the way forward in improving the quality, timeliness, and performance of the personnel security vetting process while incorporating new capabilities and approaches. This effort will require changes to existing policies and, potentially, the statutes governing those policies.

Hearing Date: 6 March 2018
Committee: SSCI
Member: Senators Burr and Warner
Witness: ODNI/NCSC, Mr. Brian D.
Info Current as of: July 2, 2018

Question 3: Reciprocity. Security Executive Agent Directive 4 on reciprocity contains an Appendix C that allows agencies substantial latitude in levying additional requirements before accepting a clearance. The SecEA provides data on reciprocity for the Intelligence Community (IC) pursuant to Sec. 504 of the *Intelligence Authorization Act for Fiscal Year 2014,* but not the rest of government.

Answer: Security Executive Agent Directive (SEAD) 4, *National Security Adjudicative Guidelines*, Appendix C, identifies exceptions to the adjudicative guidelines. These exceptions are defined as "an adjudicative decision to grant initial or continued eligibility for access to classified information ... despite failure to meet the full adjudicative or investigative standards." Appendix C lists the specific exceptions: Waiver, Condition, Deviation, or Out of Scope. While the existence of an exception in a national security determination can affect the application of reciprocity, the cited SEAD and appendix do not specifically address reciprocity.

NCSC has drafted SEAD 7, *Reciprocity of Background Investigations and National Security Adjudications.* This directive will provide reciprocity guidance and procedures for government-wide use. The requirements of 50 U.S.C. 3341(b, d), and E.O. 13467, as amended, serve as the basis for the DNI to provide reciprocity guidance for agencies. The draft SEAD has cleared internal ODNI review and is currently in the formal OMB policy coordination process.

Question 3a: As the SecEA, can you please detail what additional requirements IC and non-IC agencies require, by agency, at each clearance level?

Answer: The requirements for secret and top secret clearance reciprocity are the same for IC and non-IC agencies and are consistent with OMB and Intelligence Community Policy Guidance. The SecEA issued E/S 01074, "Executive Order 13467 (as amended) and Reciprocal Recognition of Existing Personnel Security Clearances," dated October 1, 2008. This memorandum endorses the guidance provided in the OMB memorandum. SEAD 7, when issued, will standardize policies and procedures for individuals eligible for access to classified information or eligible to hold a sensitive position across the Executive Branch.

Question 3b: As the SecEA, can you please provide data on the time it takes to for both government and industry personnel at the same level (e.g., SECRET, TOP SECRET, SCI) to transfer a clearance from an IC agency to an agency beyond the IC?

Answer: Currently, the SecEA does not capture clearance cross-over timeliness from the IC to non-IC agencies as reciprocity data is not collected from agencies outside of the IC. SecEA's reciprocity reporting for the whole of government is pending issuance of SEAD 7. Data from current reporting is limited to the IC, and the cases are Top Secret or Top Secret/SCI. In fiscal year 2017, the average IC processing time for reciprocity was 8.2 days. Once SEAD 7 is issued, it will provide standardized metrics requirements for IC and non-IC agencies.

Question 3c: Why is it possible for clearance delays to exist within an agency when a cleared individual, either government or contractor, switches projects within the same agency?

Answer: Many variables can affect clearance transfers for government employees and contractors. An individual may have a security clearance that is ineligible for reciprocity, the access may not be at the correct

level for the new position, or there may be suitability aspects of the position that require review of the original access determination.

Hearing Date: 6 March 2018
Committee: SSCI
Member: Senators Burr and Warner
Witness: ODNI/NCSC, Mr. Brian D.
Info Current as of: July 2, 2018

Question 4: Government v. Contractor Personnel.

Question 4a: Under existing policy, is a contractor who is "out of scope" for her background investigation treated differently than a government employee who is "out of scope," when moving jobs or contracts? If so, please describe how this treatment differs.

Answer: While the personnel security vetting process is very similar for contractors and government employees, the process is the same for out of scope background investigations between contractors and government personnel. However, individual circumstances and position requirements can impact security determinations. An "out of scope" background investigation can impact eligibility for reciprocity. A contractor with an out of scope background investigation could potentially move from one contract to another with the same sponsoring agency, but may not be accepted on a contract sponsored by another agency. Likewise, a government employee with an out of scope background investigation may be eligible to change jobs within their agency, while their clearance may not be accepted as part of a transfer to another agency. Suitability for employment or fitness for a position may also be a consideration.

Question 4b: Can an agency have one policy for use of the polygraph for its cleared government population and a different policy for its contractor community? If so, please provide an example.

Answer: Yes. The application of polygraph in the national security vetting process is governed by SEAD 2, *Use of Polygraph in Support of Personnel Security Determinations for Initial or Continued Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position.* Consistent with that directive, agencies structure their polygraph programs and may use any of the approved types of polygraph. While SEAD 2 does not prohibit disparate application of a given polygraph technique to government employees and contractors, NCSC would defer to individual agencies to discuss the specifics of their programs.

Hearing Date: 6 March 2018
Committee: SSCI
Member: Senators Burr and Warner
Witness: ODNI/NCSC, Mr. Brian D.
Info Current as of: July 2, 2018

Question 5: Transparency. The ODNI's most recent report on security clearance determinations was marked FOUO, in contrast to the previous version of this report, which was only UNCLASSIFIED.

Question 5a: Can you please explain what caused the change in the handling caveat?

Answer: Yes. The most recent report provided data in greater detail than in prior reports. Due to the sensitivity of the data presented, as well as the potential benefit possession of that data would provide to adversaries, a determination was made that report would be marked FOUO.

Hearing Date: 6 March 2018
Committee: SSCI
Member: Senators Burr and Warner
Witness: ODNI/NCSC, Mr. Brian D.
Info Current as of: July 2, 2018

Question 6: Clearance Portability. Is there a reason why the government cannot treat security clearances like a 401(k) that travels with the person, rather than holding the clearances at a particular government agency?

Answer: The government actually does treat security clearances in a manner very similar to a 401(k). Clearances are granted and managed by a sponsoring agency. Sponsorship includes managing the security clearance determination, reporting requirements, continuous evaluation, training, and other oversight responsibilities. While sponsorship rests with a single agency, current reciprocity guidelines direct D/As to reciprocally accept the national security determination and/or the background investigation of an individual if it is of a similar type and is within proscribed age limits. D/As are required to check for the existence of a valid background investigation prior to requesting a new one and to utilize a favorable national security determination to meet a national security access requirement. D/As are also required to document background investigations and adjudications in one of the national databases. Thus, an individual's security clearance is accessible and transportable within the existing personnel security vetting process. The issuance of SEAD 7 will support consistent application of reciprocity.

Hearing Date: 6 March 2018
Committee: SSCI
Member: Senator Wyden
Witness: ODNI/NCSC, Mr. Brian D.
Info Current as of: July 2, 2018

Question 1: Transparency. The ODNI released to the public the 2015 Annual Report on Security Clearance Determinations.

Question 1a: Does the ODNI intend to release the 2016 and subsequent reports?

Answer: Yes and did so on the ODNI's website in March of this year.

Question 1b: If not, why not?

Answer: N/A

Hearing Date: 6 March 2018
Committee: SSCI
Member: Senator Wyden
Witness: ODNI/NCSC, Mr. Brian D.
Info Current as of: July 2, 2018

Question 2: Reducing the Number of Cleared Positions. Please describe progress made in reducing the total number of government positions requiring a security clearance and lowering the clearance level for positions that do require clearances. In which departments, agencies, and offices have there been the most progress, and where has there been the least progress? Are there target goals to reduce the number of positions requiring a clearance? If yes, what current processes are in place for achieving any of these goals?

Answer: The SecEA initiated actions to better manage the size of the cleared national security population. On an ongoing basis, the SecEA reminds D/A heads to review and validate individuals' need for access to classified information. As a result of the SecEA's coordination with agency heads, the eligible national security population has decreased from approximately 5.1 million on October 1, 2013, to roughly 4.0 million on October 1, 2017 – approximately a 20% decrease in the size of the cleared population. The intent is to ensure the national security population is "right-sized," not simply reduced.

The Department of Defense (DoD) has the largest population of personnel with national security eligibility. A majority of the reduction in the national security population resulted from data integrity efforts at DoD that removed personnel who were no longer affiliated with DoD or no longer required national security eligibility.

There are no target goals for security clearances. Rather, the approach seeks to ensure that the Executive Branch has the correct number of personnel with the appropriate security clearances. In support of these efforts the SecEA and the SuitEA jointly revised Title 5 Code of Federal Regulations Part 732 (5 CFR 732), "National Security Positions," and reissued it as 5 CFR 1400, "Designation of National Security Positions in the Competitive Service, and Related Matters." This effort provided greater clarity for D/As in classifying positions requiring national security eligibility. The OPM Position Designation Tool was revised to incorporate the guidance in 5 CFR 1400, and all Executive Branch D/As were required to review existing position designations using the 5 CFR 1400 standards. These efforts seek to ensure that Executive Branch positions are properly designated and that they validate requirements for national security eligibility. The SecEA continues efforts to ensure there is a sufficient number of individuals with the appropriate clearances to meet mission requirements while ensuring unnecessary clearances are not maintained.

Hearing Date: 6 March 2018
Committee: SSCI
Member: Senator Wyden
Witness: ODNI/NCSC, Mr. Brian D.
Info Current as of: July 2, 2018

Question 3: Whistleblowers. On June 18, 2014, Senator Grassley and I wrote the DNI about the potential impact of continuous monitoring and continuous evaluation on whistle blower protections. On July 25, 2014, the DNI responded that "some agencies" were training investigators and that the National Insider Threat Task Force had issued guidance emphasizing legal protections afforded whistleblowers. The DNI further wrote that "the Inspector General of the Intelligence Community, in coordination with the Intelligence Community Inspectors General Forum, is currently examining the potential for internal controls that would ensure whistleblower-related communications remain confidential, while also ensuring the necessary UAM [user activity monitoring] occurs." Please detail any guidance, mechanisms, or procedures related to the controls the Intelligence Community and each of its component entities have implemented to ensure that any security-related personnel monitoring does not compromise the confidentiality of whistleblower-related communications.

Answer: On May 17, 2018, Michael Atkinson was sworn in as the second Senate confirmed Inspector General of the Intelligence Community (IC IG). Since that time, Mr. Atkinson has been reviewing the data available to him regarding the IC IG whistleblowing program and, also, the Intelligence Community Inspectors General Forum (IC IG Forum). With respect to this specific question, he has not located records establishing that the Forum undertook an examination of internal controls to ensure whistleblower-related communications remain confidential, while also ensuring the necessary user activity monitoring (UAM) occurs. During his confirmation process, Mr. Atkinson committed to undertake, in coordination with the IC IG Forum, an immediate review of whistleblower complaints being handled currently by the IC IG and other IC IG Forum members to ensure they are receiving appropriate resources, attention, and priority. The IC IG will also work with the ODNI and the IC IG Forum to identify best practices and procedures governing UAM to enable and encourage lawful whistleblowing while respecting the required balance with insider threat monitoring.

The National Insider Threat Task Force (NITTF) incorporates the importance of privacy, civil rights and civil liberties protections into all training and guidance materials, as well as all of its briefings and presentations. Although whistleblower protections were not uniformly addressed separately in earlier documentation, modifications were made within the past few years to do so explicitly in subsequent materials. NITTF has an active partnership with the Defense Security Service's Center for the Development of Security Excellence to develop Insider Threat training materials for the executive branch and these materials also incorporate this guidance. The criticality of Insider Threat Programs incorporating these protections is grounded in Executive Order 13587 and the National Insider Threat Policy. Examples of these NITTF products include: Hub Operations Course; 2013 Guide to Accompany the National Insider Threat Policy and Minimum Standards; 2016 Protect Your Organization from the Insider Out: Government Best Practices; and the 2017 Insider Threat Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards. The most recent presentation given by the Director of the NITTF was at the 25 April 2018 DARPA Defense Industry Security Symposium in San Diego where he stated, "Your leadership and insider threat program personnel need to consult with legal counsel, privacy and civil liberties and whistleblower protection officers from the outset of the insider threat program. They should be an ongoing part of any insider threat program discussions."