

Calendar No. 610

113TH CONGRESS }
2d Session }

SENATE

{ REPORT
113-283 }

ENHANCED SECURITY CLEARANCE ACT OF
2014

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

TO ACCOMPANY

S. 1618

TO ENHANCE THE OFFICE OF PERSONNEL MANAGEMENT BACK-
GROUND CHECK SYSTEM FOR THE GRANTING, DENIAL, OR REV-
OCATION OF SECURITY CLEARANCES OR ACCESS TO CLASSI-
FIED INFORMATION OF EMPLOYEES AND CONTRACTORS OF THE
FEDERAL GOVERNMENT



DECEMBER 2, 2014.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE

49-010

WASHINGTON : 2014

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

THOMAS R. CARPER, Delaware *Chairman*

CARL LEVIN, Michigan	TOM COBURN, Oklahoma
MARK L. PRYOR, Arkansas	JOHN McCAIN, Arizona
MARY L. LANDRIEU, Louisiana	RON JOHNSON, Wisconsin
CLAIRE McCASKILL, Missouri	ROB PORTMAN, Ohio
JON TESTER, Montana	RAND PAUL, Kentucky
MARK BEGICH, Alaska	MICHAEL B. ENZI, Wyoming
TAMMY BALDWIN, Wisconsin	KELLY AYOTTE, New Hampshire
HEIDI HEITKAMP, North Dakota	

GABRIELLE A. BATKIN, *Staff Director*

JOHN P. KILVINGTON, *Deputy Staff Director*

MARY BETH SCHULTZ, *Chief Counsel*

LAWRENCE B. NOVEY, *Chief Counsel for Governmental Affairs*

TROY H. CRIBB, *Chief Counsel for Governmental Affairs*

KEITH B. ASHDOWN, *Minority Staff Director*

CHRISTOPHER J. BARKLEY, *Minority Deputy Staff Director*

ANDREW C. DOCKHAM, *Minority Chief Counsel*

MARK K. HARRIS, *Minority U.S. Coast Guard Detailee*

LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 610

113TH CONGRESS }
2d Session }

SENATE

{ REPORT
{ 113-283

ENHANCED SECURITY CLEARANCE ACT OF 2014

DECEMBER 2, 2014.—Ordered to be printed

Mr. CARPER, from the Committee on Homeland Security and
Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 1618]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 1618), to enhance the Office of Personnel Management background check system for the granting, denial, or revocation of security clearances or access to classified information of employees and contractors of the Federal Government, having considered the same, reports favorably thereon with an amendment in the nature of a substitute and recommends that the bill, as amended, do pass.

CONTENTS

	Page
I. Purpose and Summary	1
II. Background and Need for the Legislation	2
III. Legislative History	11
IV. Section-by-Section Analysis	11
V. Evaluation of Regulatory Impact	12
VI. Congressional Budget Office Cost Estimate	13
VII. Changes in Existing Law Made by the Bill, as Reported	14

I. PURPOSE AND SUMMARY

S. 1618 seeks to make the nation more secure by requiring that federal personnel who have security clearances or who hold sensitive agency jobs will have their background information checked more frequently than is done now. The government periodically re-investigates the background information of these individuals, though the required schedule for these periodic re-investigations is frequently not met, and the sometimes lengthy periods between re-investigations creates vulnerability. This bill would address that vulnerability by supporting the government's efforts to clear the backlog of periodic re-investigations and by requiring randomly

timed automated background checks during the interim between the periodic reinvestigations. Taken together, these steps would enable the quicker discovery of information that may call into question the trustworthiness of personnel with clearances or in sensitive positions.

II. BACKGROUND AND NEED FOR THE LEGISLATION

Processes for vetting government personnel for security clearances and sensitive positions. Because unauthorized disclosure of classified information can cause damage to national security and loss of human life, federal personnel—including civilian employees, military personnel, and employees of contractors and grantees—are allowed access to classified information only after the government conducts a background investigation and issues them a security clearance.¹ For classified national security information, the levels of security clearance—“Top Secret,” “Secret,” and “Confidential”—correspond to the degree of sensitivity of the classified information to which the individual may have access.² To indicate access to sensitive nuclear information and materials, “Q” clearances and “L” clearances are issued, with Q clearances allowing access to the more highly sensitive level.³ Another category of security clearances allow access to “Controlled Access Programs,” including “Sensitive Compartmented Information,” which involves intelligence matters and is particularly sensitive.⁴

Moreover, the head of an agency is required to designate positions within the agency as “sensitive positions” if an individual occupying a position could bring about “a material adverse effect on the national security.”⁵ Most sensitive career civil-service positions and some others are categorized among three levels of sensitivity: “Noncritical-Sensitive,” “Critical-Sensitive,” and “Special-Sensitive.”⁶

The vetting of government personnel generally involves two distinct steps: investigation and adjudication. A security investigation begins when the individual, at the request of the sponsoring agency, submits an application in which the individual provides detailed information on a broad range of topics, including: personal history, identity of relatives and friends, foreign contacts and activities, criminal and legal record, any financial or tax difficulties, use of

¹ See Exec. Ord. 12968 “Access to Classified Information” (Aug. 2, 1995) (50 U.S.C. § 3161 note).

² See Exec. Ord. 13526 “Classified National Security Information” (Dec. 29, 2009) (50 U.S.C. § 3161 note).

³ See U.S. Department of Energy, Order DOE O 472.2, “Personnel Security” (Approved: July 21, 2011), <https://www.directives.doe.gov/directives-documents/400-series/0472.2-BOrder>, <https://www.directives.doe.gov/directives-documents/400-series/0472.2-BOrder/@@download/file>; U.S. Nuclear Regulatory Commission, Information Security (Last Reviewed/Updated October 31, 2013), <http://www.nrc.gov/security/info-security.html>.

⁴ See Office of the Director of National Intelligence, Number 704.1, Intelligence Community Policy Guidance, Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information (ICPG 704.1, Oct. 2, 2008), http://www.ncix.gov/publications/policy/docs/ICPG_704-1_Investigative%20Standards.pdf.

⁵ See Exec. Ord. 10450 (April 27, 1953) (5 U.S.C. § 7311 note).

⁶ See 5 C.F.R. § 732.101 (The requirement to designate sensitive positions at one of these three levels of sensitivity applies to position in the competitive service (*i.e.*, positions filled according to the Office of Personnel Management’s competitive-hiring regulations) and to Senior Executive Service positions filled by career appointment, and agencies may apply the requirement to other positions); Office of Personnel Management, Position Designation Tool, Position Designation of National Security and Public Trust Positions (October 2010), <http://www.opm.gov/investigations/background-investigations/position-designation-tool/oct2010.pdf>.

drugs and alcohol, and other matters.⁷ Then, using the information provided by the applicant, a background investigation is conducted. The Office of Personnel Management (OPM) conducts the great majority of the investigations, though several agencies, many of which are in the Intelligence Community, are authorized to conduct their own.⁸ OPM hires contractors to conduct much of the information collection, and other agencies also use a mix of contractors and federal employees to gather the information needed for a background investigation.⁹

The degree of scrutiny of an individual's background will depend on the level of risk or sensitivity of the information or position to which the individual may be granted access. The background investigation may include reviews of the individual's criminal history, any terrorist activity, credit issues, and foreign activities and influence, and may also include interviews of the subject, employers, and social references.¹⁰ Following the background investigation comes the adjudication stage, in which the sponsoring agency assesses the information collected and determines whether to grant to the individual a security clearance or allow the individual to occupy the sensitive position.

Individuals with security clearances may be the subject of reinvestigation any time there is reason to believe the individual may no longer meet the standards for the clearances, but cleared individuals are also supposed to be the subject of a periodic reinvestigation a specified number of years after the last investigation. The frequency of periodic reinvestigation was originally established government-wide in 1997 with three different periods for the three levels of security-clearance access,¹¹ and the frequency has been standardized with a uniform reinvestigation requirement of every five years, regardless of the level of access.¹²

Moreover, employees in Special-Sensitive and Critical-Sensitive positions must undergo reinvestigation at least every five years under current regulations, and some agencies require reinvestigations for employees in Noncritical-Sensitive positions every 10 years. The regulations applicable to these categories of sensitive positions in the career civil service are now under review, and the requirements for reinvestigation may be changed when revised regulations are issued.¹³

Recent high-profile incidents focused attention on the need to strengthen security-related vetting processes. Several high-profile

⁷ See OPM, Standard Form 86, "Questionnaire for National Security Positions (Revised December 2010).

⁸ See Office of Management and Budget, "Suitability and Security Processes Review: Report to the President," conducted by the Suitability and Security Clearance Performance Accountability Council (February 2014) ("120-day Suitability and Security Report"), at pages 2-3, <http://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf>.

⁹ See *id.*

¹⁰ See *id.*

¹¹ The requirement for periodic reinvestigations established in 1997 was: every 5 years for a Top Secret clearance or for access to sensitive compartmentalized information; every 10 years for a Secret clearance, and every 15 years for a Confidential clearance. See *id.*, at page 2. This minimum frequency was established in Federal Investigative Standards issued in 1997 pursuant to section 3.4(c) of Exec. Ord. 12968, note 1 above.

¹² See Beth Cobert, Deputy Director for Management at the Office of Management and Budget and Chair of the Suitability and Security Clearance Performance Accountability Council, "Progress on Security and Suitability," posted by Beth Cobert (Sept. 16, 2014), <http://www.whitehouse.gov/blog/2014/09/16/progress-security-and-suitability>.

¹³ See 5 C.F.R. § 732.203; 78 Fed. Reg. 31847 (May 28, 2013); 75 Fed. Reg. 77783, 77784-77785 (Dec. 14, 2010).

crimes committed in recent years by individuals with security clearances have highlighted weakness in our processes for vetting cleared federal personnel and demonstrated the urgent need to strengthen these processes:

- On November 5, 2009, U.S. Army Major Nidal Malik Hasan, while holding a Secret security clearance, shot and killed 13 people and wounded 43 others at Fort Hood, Texas.¹⁴

- During 2009 and 2010, an Army intelligence analyst, then named Bradley Manning, stole and publicly leaked enormous quantities of classified documents regarding military operations in Iraq and Afghanistan.¹⁵

- During June 2013, computer systems administrator Edward Snowden leaked to the news media enormous quantities of National Security Agency classified documents that he obtained while working for intelligence contractors Dell and Booz Allen, in what is said to be the most massive and damaging intelligence leak in our history.¹⁶

- Most recently, on September 16, 2013, Aaron Alexis, fatally shot 12 U.S. Navy civilian and contractor employees and wounded several others in a mass shooting inside the Washington Navy Yard in Washington, D.C.¹⁷ At the time of the shooting, and despite a history of arrests and other troubling behavior, Alexis was employed by a Navy contractor and held a Secret-level security

¹⁴See U.S. Senate Committee on Homeland Security and Governmental Affairs, “A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government’s Failure to Prevent the Fort Hood Attack,” a special report by Joseph I. Lieberman, Chairman, and Susan M. Collins, Ranking Member (Feb. 3, 2011), <http://www.hsgac.senate.gov/download/fort-hood-report>; Hearing before the Senate Committee on Homeland Security and Governmental Affairs, 111th Cong., 1st Sess., “The Fort Hood Attack: A Preliminary Assessment,” S.Hrg. 111-810 (November 19, 2009), <http://www.gpo.gov/fdsys/pkg/CHRG-111shrg56145/pdf/CHRG-111shrg56145.pdf>; U.S. Department of Defense, Report of the DoD Independent Review, “Protecting the Force: Lessons from Fort Hood” (January 2010), at pages 12–13, http://www.defense.gov/pubs/pdfs/DOD-ProtectingTheForce-Web_Security_HR_13Jan10.pdf; Department of Defense, “Internal Review of the Washington Navy Yard Shooting: A Report to the Secretary of Defense” (November 20, 2013) (“DoD Internal Review”), at pages 15–16, <http://www.defense.gov/pubs/DoD-Internal-Review-of-the-WNY-Shooting-20-Nov-2013.pdf>.

¹⁵See U.S. Army, “Army to transfer Manning to new Leavenworth correctional facility,” by Donna Miles, American Forces Press Service (April 19, 2011), <http://www.army.mil/article/55211/army-to-transfer-manning-to-new-leavenworth-correctional-facility/>; U.S. Army, “Army charges Manning with leaking intelligence,” by Dave Vergun (Feb. 23, 2012), http://www.army.mil/article/74417/Army_charges_Manning_with_leaking_intelligence/; U.S. Army, “Manning guilty of 20 specifications, but not ‘aiding the enemy’”, by David Vergun, Gary Sheftick (July 26, 2013), http://www.army.mil/article/108143/Manning_guilty_of_20_specifications_but_not_aiding_enemy/. In April 2014, Manning’s name was legally changed to Chelsea Elizabeth Manning, at Manning’s request. See Ernesto Londono, “Convicted leaker Bradley Manning changes legal name to Chelsea Elizabeth Manning,” Washington Post (April 23, 2014), http://www.washingtonpost.com/world/national-security/convicted-leaker-bradley-manning-changes-legal-name-to-chelsea-elizabeth-manning/2014/04/23/e2a96546-cb1c-11e3-a75e-463587891b57_story.html.

¹⁶See “Safeguarding our Nation’s Secrets: Examining the Security Clearance Process,” joint hearing before the Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce and the Subcommittee on Financial and Contracting Oversight, Senate Committee on Homeland Security and Governmental Affairs, 113th Cong, 1st Sess. (June 20, 2013), S. Hrg. 113-316; testimony of James R. Clapper, Director of National Intelligence, “Open Hearing: Current and Projected National Security Threats Against the United States,” before the Senate Intelligence Committee, January 29, 2014, <http://www.intelligence.senate.gov/hearings.cfm?hearingid=138603a26950ad873303535a630ec9c9&witnessid=138603a26950ad873303535a630ec9c9-0-1>, unofficial transcript at http://www.washingtonpost.com/world/national-security/transcript-senate-intelligence-hearing-on-national-security-threats/2014/01/29/b5913184-8912-11e3-833c-33098f9e5267_story.html. See also, Mark Hosenball, “Snowden downloaded NSA secrets while working for Dell, sources say,” Reuters (Aug. 15, 2013), <http://www.reuters.com/article/2013/08/15/usa-security-snowden-dell-idUSL2NOGF11220130815>.

¹⁷See DoD Internal Review, note 14 above; “), <http://www.defense.gov/pubs/DoD-Internal-Review-of-the-WNY-Shooting-20-Nov-2013.pdf>; Department of Defense, “Security from Within: Independent Review of the Washington Navy Yard Shooting” (November 2013) (“DoD Independent Review”), <http://www.defense.gov/pubs/Independent-Review-of-the-WNY-Shooting-14-Nov-2013.pdf>.

clearance, issued in March 2008 while he was in the military service.

In the periods leading up to each of these incidents, there had been warning signs about troublesome behavior by the individual involved which were not heeded or communicated to the proper authorities. During Hasan's military medical training, colleagues and superiors had expressed concern about his behavior and comments, and government officials were aware that Hasan had expressed violent, extremist sentiments.¹⁸ Manning had demonstrated instability by his many emotional and physical outbursts in the months leading up to his leaking classified documents, and had even disregarded basic security measures common to classified working environments.¹⁹ Reportedly, Snowden had been suspected of trying to break into classified computers, and changes in his behavior and work habits raised concerns when he was working for the CIA in 2007–2009.²⁰ Alexis had been arrested several times, twice involving firearms, and in the weeks before the Navy Yard shooting had been observed complaining of being followed, of hearing voices, and of being under attack by vibrations and microwaves.²¹

On October 30, 2013, in the aftermath of the Navy Yard shooting, Senators Collins, McCaskill, Ayotte, and Heitkamp introduced S. 1618, the Enhanced Security Clearance Act, to require randomly timed audits of background information for cleared personnel. The next day, on October 31, 2013, this Committee held a hearing entitled “The Navy Yard Tragedy: Examining Government Clearances and Background Checks,” at which S. 1618 was one of several topics discussed.²²

Also in the fall of 2013, the President instructed the Office of Management and Budget (OMB) to conduct within 120 days a thorough review of the suitability and security vetting procedures for civilian, military, and contractor personnel. (“Suitability” refers to being found suitable for federal employment generally; “security” refers to being found eligible to hold a sensitive national security position or to have access to classified information.²³) Having conducted the work through an interagency team,²⁴ OMB prepared

¹⁸ See U.S. Senate Committee on Homeland Security and Governmental Affairs, “A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government’s Failure to Prevent the Fort Hood Attack,” a special report by Joseph I. Lieberman, Chairman, and Susan M. Collins, Ranking Member (Feb. 3, 2011), at pages 27–39, <http://www.hsgac.senate.gov/download/fort-hood-report>.

¹⁹ See DoD Internal Review, note 14 above, at page 16.

²⁰ See Eric Schmitt, “CIA Warning on Snowden in ‘09 Said to Slip Through the Cracks,” *New York Times* (October 10, 2013), http://www.nytimes.com/2013/10/11/us/cia-warning-on-snowden-in-09-said-to-slip-through-the-cracks.html?pagewanted=all&_r=0.

²¹ See DoD Internal Review, note 14 above, at page 16.

²² Hearing before the Senate Committee on Homeland Security and Governmental Affairs, “The Navy Yard Tragedy: Examining Government Clearances and Background Checks” (October 31, 2013) (“HSGAC hearing”), <http://www.gpo.gov/fdsys/pkg/CHRG-113shrg85500/pdf/CHRG-113shrg85500.pdf>. Witnesses were: Joseph G. Jordan, Administrator, Office of Federal Procurement Policy, Office of Management and Budget; Elaine D. Kaplan, Acting Director, U.S. Office of Personnel Management; Brian A. Prioletti, Assistant Director, Special Security Directorate, National Counterintelligence Executive, Office of the Director of National Intelligence; Stephen Lewis, Deputy Director for Personnel, Industrial and Physical Security Policy, Directorate of Security Policy & Oversight, Office of Under Secretary of Defense for Intelligence, U.S. Department of Defense; and Brenda Farrell, Director, Defense Capabilities and Management, U.S. Government Accountability Office.

²³ For employment in a civilian position outside the competitive service or a position with a government contractor, the term “fitness” is generally used instead of “suitability.” See, generally, 5 C.F.R. parts 302, 731.

²⁴ The work was carried out by the Suitability and Security Clearance Performance Accountability Council (PAC), which was established by section 2.2 of Exec. Order. 13467 (June 30,

and submitted, and the President approved, the report in the winter of 2013 (“Suitability and Security Processes Review: Report to the President” (February 2014), referred to herein as the “120-day Suitability and Security Report”).²⁵

Addressing the vulnerable time-gap between periodic reinvestigations. Reviews in the aftermath of the Navy Yard shooting and the other recent incidents found that a substantial weakness in the current process arises from the time-gap between periodic reinvestigations. As the Administration’s 120-day Suitability and Security Report put it,

The current reinvestigation practices do not adequately reevaluate or appropriately mitigate risk within the security and suitability population. Lengthy periods between reinvestigations do not provide sufficient means to discover derogatory information that develops following the initial adjudication.²⁶

The events involving Alexis prior to the shooting at the Navy Yard starkly demonstrate this vulnerability. Alexis had several run-ins with law enforcement, including at least two within the period since his 2007 background investigation: an August 2008 arrest in Georgia for disorderly conduct and a September 2010 arrest in Texas for unlawfully discharging a firearm.²⁷ Moreover, the defense contractor by whom Alexis was employed at the time of the shooting was aware of indications of his mental instability, but failed to report that information to the Defense Department as required under the contract, apparently influenced by a lack of clear understanding about what must be reported.²⁸ Thus, information showing Alexis’s instability was available in police records and was known to government contractors with an obligation to report it, but no mechanism existed to adequately bring such information to the attention of the agency between periodic investigations. The DoD Independent Review found that “DoD gains little to no insight into its cleared workforce between periodic investigations” and that the Department must find a way to account for this risk.²⁹

Moreover, the schedule for periodic reinvestigations is not being met. The 120-day Suitability and Security Report found that “resource constraints lead agencies to conduct fewer than the required number of reinvestigations,”³⁰ resulting in a backlog of periodic reinvestigations for even the most sensitive populations.³¹ Of the individuals eligible for access to Top Secret classified information or to Sensitive Compartmentalized Information, roughly 22 percent of the background investigations were outdated as of March 2014, and no reinvestigation had even been requested.³²

2008) (5 U.S.C. §3161 note); and a Senior Review Panel of representatives from key security and personnel agencies drove the review and to identify recommended solutions. See 120-day Suitability and Security Report, note 8 above, at page 1.

²⁵ 120-day Suitability and Security Report, note 8 above; see also OMB press release, “Administration Releases Suitability and Security Report” (March 18, 2014), <http://www.whitehouse.gov/sites/default/files/omb/press-releases/suitability-and-security-report-press-release-03182014.pdf>.

²⁶ 120-day Suitability and Security Report, note 8 above, at page 8.

²⁷ DoD Independent review, note 17 above, at page 39.

²⁸ See HSGAC October 31, 2013 hearing, note 23 above, Lewis’s oral testimony; DoD Internal Review, note 14 above, at page 20–21, 36–37; DoD Internal Review, note 14 above, at page 20.

²⁹ DoD Independent Review, note 17 above, at page 16.

³⁰ 120-day Suitability and Security Report, note 8 above, at page 8.

³¹ *Id.*, at page 11.

³² *Id.*

During the time-gap between reinvestigations, the government relies on individuals to self-report and on others to report any relevant information. However, the requirements are not adequate, and too little reporting is being done. As noted above, the managers at the defense contractor that employed Alexis were aware of troubling behavior, but “[t]he employer’s decision not to report Alexis’ behavior appears to be influenced by a lack of awareness about what types of behaviors are considered ‘adverse’ information that must be reported (particularly those related to mental health issues).”³³ Likewise, regarding the incident involving Manning, DoD found, “In the months leading up to the unauthorized disclosure, Manning displayed behaviors indicating instability through multiple emotional and physical outbursts, expressed discontent with the Army and the Federal Government, and disregarded basic security measures common to all classified working environments.”³⁴ More generally, the 120-day Suitability and Security Report found that inadequate reporting and self-reporting is a critical and pervasive problem:

This review found that clear and consistent requirements do not exist across government for employees or contractors to report, subsequent to their being hired or granted a clearance, information that could affect their continued fitness, suitability, or eligibility for Federal employment (e.g., criminal conduct, behaviors of concern), or their eligibility to access government facilities and IT systems. Neither is there consistent guidance in place to direct contractors or contract managers in the Federal Government to report noteworthy or derogatory information regarding employees.³⁵

Recognizing the security vulnerabilities that arise from the time-gap between reinvestigations, the agencies are undertaking a number of efforts to eventually address various aspects of this problem. The government has been working to establish automated systems, referred to generally as Continuous Evaluation (CE), to check government and commercial data sources on a more frequent or even continuous basis to flag issues of concern during the period between background investigations. At this Committee’s October 31, 2013 hearing, witnesses reported that all government agencies already conduct some automated electronic record checks now,³⁶ and described the Automated Continuous Evaluation System (ACES) being developed by DoD to test, on a large population of cleared military, civilian, and contractor personnel, the concepts of conducting one-time inquiries and then moving towards providing real-time updates as soon as an arrest is posted on a law-enforcement database, for example, or when other relevant information becomes available.³⁷

The 120-day Suitability and Security Report stated that the ACES and other pilots provide compelling evidence of the benefits of the CE approach, and that CE can help address the vulnerability

³³ See DoD Internal Review, note 14 above, at page 20.

³⁴ See *id.*, at page 16.

³⁵ 120-day Suitability and Security Report, note 8 above, at page 7.

³⁶ HSGAC Hearing, note 23 above, oral testimony of Prioletti.

³⁷ HSGAC Hearing, note 23 above, oral testimony of Lewis.

arising from the years-long time-gap between periodic reinvestigations:

By identifying issues between reinvestigations, CE will more frequently evaluate employees and contractors who are eligible for access to classified information by using periodic, random, and event-driven assessments to better resolve issues or identify risks to national security.³⁸

The Report explained that CE is an ambitious undertaking—“Success of the CE program will depend on a fully-integrated solution across government, which will eliminate inefficiency and avoid the expenses of duplicative systems”³⁹—and the report also recognized the challenges and stated how much is yet to be done to reach that goal:

Implementing a system for continuous evaluation is resource intensive, and poses genuine technical and procedural challenges. Currently there is no government-wide capability, plan or design present in the investigative community to operate a data-driven architecture to collect, store, and share relevant information.⁴⁰

To help manage and track government-wide progress towards implementing the recommendations from the 120-day Suitability and Security Review, including CE, OMB recently published an implementation work plan as part of its new Cross Agency Priority Goal of “Insider Threat and Security Clearance Reform.”⁴¹ The workplan for FY2014 Quarter 3 sets out a series of ten milestones. Specifically for personnel with Top Secret or sensitive compartmented clearance, the workplan sets a December 2014 goal for having an initial CE capability for the most sensitive population, and a December 2016 goal for the entire population. The workplan includes tiered expansion by DoD of its CE capability to cover 100,000 cleared personnel by October 2014, 225,000 personnel by December 2015, 500,000 personnel by December 2016, and 1 million during 2017. Other milestones include various planning goals and other items. The workplan illustrates the Administration’s commitment to achieving a government-wide CE capability, as well as the length of the road ahead.

To address the reinvestigation backlog itself, the 120-day Suitability and Security Report includes recommendations to reduce the backlog using a “risk-based approach” that would “identify high risk populations through the use of automated records checks (*e.g.*, derogatory credit or criminal activity) and prioritize overdue investigations based on the risk posted by job responsibilities and access.”⁴²

With respect to self-reporting and reporting by others during the period between reinvestigations, the 120-day Suitability and Security Report set forth a multi-stage planning process. Uniform reporting requirements applicable to employees across the executive

³⁸ 120-day Suitability and Security Report, note 8 above, at page 9.

³⁹ *Id.*

⁴⁰ *Id.*

⁴¹ Cross Agency Priority Goal Quarterly Progress Update, “Insider Threat and Security Clearance Reform,” FY2014 Quarter 3, Work Plan: Implement Continuous Evaluation, <http://www.performance.gov/node/3407/view?view=public#progress-update>.

⁴² 120-day Suitability and Security Report, note 8 above, at pages 11–12.

branch must first be developed and issued, followed by training for both employees and supervisors. Moreover, to establish uniform reporting requirements applicable to government contractors, the Office of Federal Procurement Policy will need to propose and issue changes to the Federal Acquisition Regulations that would “impose those applicable reporting requirements on contractors and to ensure that enforcement and accountability mechanisms are in place.”⁴³

S. 1618, to require randomly timed automated record checks during the time-gap between reinvestigations. As discussed, plans are being developed and implemented to address the three major aspects of time-gap between reinvestigations—

- Development and implementation of CE capabilities, which can provide prompt or real-time access to relevant data during the period between reinvestigations.
- A program to apply a risk-based approach to identify high-risk populations while eliminating the backlog of overdue reinvestigations.
- Plans to foster more reliable self reporting and reporting by managers and colleagues when troubling information becomes evident.

Even with the current efforts, full implementation of these efforts will be years in the future. To support these ongoing efforts and to strengthen the security process while long-term solutions are being put into place, the Committee decided that every individual with a security clearance or eligible to hold a sensitive position should be covered by a program of random automated record checks, as provided under S. 1618.

As noted, S. 1618 was introduced soon after the mass shooting at the Washington Navy Yard. Over the subsequent several months, the responsible agencies under the leadership of the PAC conducted in-depth reviews and developed strategies and plans, summarized in the 120-day Suitability and Security Report, to reform the processes to improve decisionmaking and reduce risk in the vetting of federal personnel, particularly with regard to eligibility for security clearances and for holding sensitive positions. Over the past several months, staff for the bill sponsors have engaged in detailed discussions with agency officials involved in the preparation of the Report and implementation of its recommendations, and, informed by those discussions, the sponsors modified the legislation to ensure that it is consistent with, and supportive of, the agencies’ ongoing plans. That modified language constitutes the substitute amendment submitted to, and approved by, the Committee.

S. 1618, as amended, would reform the security programs for federal employees, military personnel, and employees of contractors in several key ways. The central element of the legislation is to require each agency to establish an Enhanced Personnel Security Program under which individuals with security clearances or who are eligible to occupy sensitive positions would be the subject of randomly timed automated record checks. To avoid drawing resources away from the ongoing efforts to address the backlog in reinvestigations, the full requirements regarding enhanced personnel

⁴³*Id.*, at pages 7–8.

security programs would not go into effect until the backlog is eliminated, or until five years pass since enactment, whichever comes first.

For this initial period, S. 1618 codifies the recommendation in the 120-day Suitability and Security Report stating that the Director of National Intelligence must develop and implement a plan to eliminate the backlog and that this plan should use a risk-based approach to prioritize reinvestigations. To achieve a prompt reduction in vulnerability while this backlog is being eliminated, the bill requires that every individual who has a security clearance or who is eligible to hold a sensitive position would be placed into a pool of individuals subject to a one-time automated record check. It is expected that the agencies will require at least five years to address the reinvestigation backlog. During this period, the randomly timed audits will insert a critical security component for the population who have not yet been the subject of a reinvestigation.

Once the backlog has been addressed or five years have passed, whichever comes first, the full requirements of the Enhanced Personnel Security Program will go into effect. The Director of National Intelligence will then direct each agency to provide enhanced security review of all individuals who have security clearances or eligibility to occupy sensitive positions. Such a program must integrate relevant information from various sources, including government and commercial data sources, consumer reporting agencies, and social media, including the types of information that are relevant for consideration in a background investigation. Any individual covered by the enhanced personnel security program will then be subject to two randomly timed audits every five years.

The audits will increase the likelihood that troubling information about cleared personnel or employees in sensitive positions will be promptly discovered by the responsible agency. Moreover, by making covered individuals aware (as well as making those, like managers, who are obligated to report, aware) that the individual's background information will be audited and that the timing of the audits is unpredictable, the legislation would create a powerful incentive for the individual to promptly self-report (and for others, like managers, to report) before the audit occurs. S. 1618 would thus strengthen the national security helping agencies to promptly learn of incidents or changed circumstances indicating that an individual is no longer trustworthy enough to be eligible for a security clearance or a sensitive government position.

S. 1618 provides that random audits would not be required if more frequent automated checks of governmental and commercial records and data are being conducted with respect to the individual. This exemption for individuals who are the subject of more frequent automated checks is a key component of the program. This provision would phase out the random audit requirement as individuals are placed under CE or similar automated programs, because relevant data regarding such individuals would be obtained more frequently or in real-time. The enhanced personnel security program under S. 1618 in this way dovetails with CE as it is being implemented, thereby preventing duplication of effort but enabling the automated record checks to apply with respect to individuals who are not covered by the more rigorous CE systems in the future.

S. 1618 thus increases the likelihood that troubling behavior or other derogatory information about personnel with security clearances or eligibility to occupy sensitive positions will be identified in the current system. It also provides a safety net should CE not be fully implemented or be delayed. S. 1618 does not replace the current process, but rather strengthens the current system and provides a safety net while these broader reforms, like CE, are instituted.

III. LEGISLATIVE HISTORY

On October 30, 2013, Senators Collins, McCaskill, Ayotte, and Heitkamp introduced S. 1618, the Enhanced Security Clearance Act of 2013, which was referred to the Homeland Security and Governmental Affairs Committee. The Committee considered S. 1618 at a business meeting on July 30, 2014.

Senators McCaskill and Heitkamp offered a substitute amendment containing a number of changes based on staff discussions with representatives of OMB and other agencies involved in preparing the 120-day Suitability and Security Review. Changes in the legislation made by the substitute amendment include—(1) deferring the requirement that enhanced security programs be implemented until after the agencies have eliminated the backlog in reinvestigations (not to exceed five years after enactment); (2) assigning to the Director of National Intelligence the responsibility for directing the implementation of a program to provide enhanced security review by each agency; and (3) making the enhanced personnel security program applicable to individuals eligible to hold a sensitive position in the government, as well as to individuals with security clearances. In addition, Senator McCaskill offered an amendment to the title of the bill.

The Committee approved the McCaskill-Heitkamp substitute amendment and the McCaskill amendment to the title of the bill, both by voice vote. The Committee then ordered S. 1618, as amended, reported favorably by voice vote, with Senator Coburn asking to be recorded “present.” Senators present for all three votes were: Carper, Levin, Landrieu, McCaskill, Begich, Baldwin, Coburn, Johnson, and Ayotte.

IV. SECTION-BY-SECTION ANALYSIS OF THE BILL, AS REPORTED

Section 1—Short title

This section states that the short title of the bill is the “Enhanced Security Clearance Act of 2014.”

Section 2—Enhancing Government Personnel Security Programs

Subsection (a)—Definitions

This subsection defines two terms:

- The term “covered individual” is defined to mean an individual who has been determined eligible for access to classified information or to hold a sensitive position.
- The term “periodic reinvestigations” is defined to mean investigations conducted periodically, with a frequency as required by the Director of National Intelligence, for the purpose of updating a previously conducted security background investigation.

Subsection (b)—Resolution of backlog of overdue periodic re-investigations

This subsection directs the Director of National Intelligence to develop and implement a plan to eliminate the backlog of overdue periodic investigations of covered individuals. In developing this plan, the Director must use a risk-based approach to identify high-risk populations and to prioritize investigations. During this time, each covered individual would be included in a pool subject to one random audit.

Subsection (c)—Enhanced Security Clearance Programs

This subsection adds a new section 11001 to title 5, United States Code, which would require that an Enhanced Personnel Security Program be established at each agency. In addition, the subsection would provide that the Inspector General of each agency must conduct at least one audit of the agency's enhanced personnel security program.

The subsection includes the following specific requirements with respect to the Enhanced Personnel Security Programs:

- The Director of National Intelligence must direct each agency to provide for enhanced security reviews of all covered individuals following the elimination of the backlog of reinvestigations or by five years after enactment of the bill, whichever comes first.
- The Enhanced Security Program at each agency must require at least two random automatic record checks (audits) in each five-year period for each covered individual who is employed by the agency or by a contractor for the agency, unless an individual is covered by Continuous Evaluation or a similar program that provides for automated record checks regarding the individual more frequently than twice in each five-year period.
- The Enhanced Security Program of each agency must integrate relevant information from various sources, including government sources, publicly available and commercial data sources, consumer reporting agencies, social media, and such other sources as are determined by the Director of National Intelligence.
- The head of each agency must ensure that each covered individual is adequately advised of the types of information the individual is required to report. A review of the information relating to the individual may not be conducted until more than 120 days after the individual receives the notification.
- The Director of National Intelligence also must issue guidance defining minor financial or mental health issues in accordance with this section of the bill.

Beginning two years after the date of implementation of the Enhanced Personnel Security Program at each agency, the Inspector General of the agency must conduct at least one audit to assess the effectiveness and fairness of the system, in accordance with performance measures and standards established by the Director of National Intelligence.

V. EVALUATION OF REGULATORY IMPACT

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of S. 1618. The Congressional Budget Office

states that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandate Reform Act and would impose no costs on state, local, or tribal governments, or private entities. The enactment of this legislation will not have significant regulatory impact.

VI. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

S. 1618—Enhanced Security Clearance Act of 2014

S. 1618 would require federal agencies to develop an enhanced personnel security program that would conduct interim reviews of certain types of information (primarily electronic records) between regularly scheduled full background investigations for individuals with security clearances or who hold sensitive positions that might affect national security (some positions are designated as sensitive but do not require security clearances). Based on guidance from the Office of the Director of National Intelligence (ODNI), agencies would be required to check certain types of information—such as criminal, financial, and social media records—not less than twice every five years to ensure the continued suitability of individuals to hold security clearances or to remain in sensitive positions.

Enacting S. 1618 would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply.

Conducting the required checks and incorporating newly acquired information into the security records of employees would increase the costs to certain federal agencies, subject to appropriation of the necessary funds. However, the bill would not require the program to be implemented until the earlier of five years after enactment of the bill or such time as the current backlog in periodic security reinvestigations is eliminated. Periodic reinvestigations are background checks of individuals who have previously had background investigations and are supposed to occur every five years. Because there has been a significant backlog in such investigations for many years, CBO anticipates that the new program would not be implemented until after 2019; therefore, the costs of implementing the bill would be negligible over the 2015–2019 period.

Although CBO does not have enough information to provide a precise estimate of the costs of implementing S. 1618 after 2019, the cost of conducting the kinds of record checks that would be required by the bill and the large number of employees who would probably be affected indicates that those costs would be significant. S. 1618 would require such checks to be completed twice every five years. CBO expects that the records checks would require a level of effort roughly equivalent to that of a basic National Agency check, which is a check of certain government records, including federal investigative records. Such checks currently cost about \$100 each.

About 5 million people currently hold security clearances and an unknown additional number hold positions that do not require security clearances but are deemed sensitive for the purpose of national security. However, both the ODNI and the Department of Defense (DoD) are developing programs under current law to continually evaluate certain personnel for their fitness to hold security clearances or to remain in sensitive positions. Personnel subject to those programs would be exempted from the checks required under

S. 1618. Although no data are available on the number of people the ODNI's program would cover, DoD's program is expected to apply to approximately 1 million employees by the end of 2017. On that basis, the costs of implementing S. 1618 would probably be in the low hundreds of millions of dollars a year after 2019.

S. 1618 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would not affect the budgets of state, local, or tribal governments.

The CBO staff contact for this estimate is Jason Wheelock. The estimate was approved by Theresa Gullo, Deputy Assistant Director for Budget Analysis.

VII. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by S. 1618, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

UNITED STATES CODE

TITLE 5—GOVERNMENT ORGANIZATION AND EMPLOYEES

* * * * *

PART III—EMPLOYEES

SUBPART A—GENERAL PROVISIONS

Chap.		Sec.
21. Definitions		2101
* * * * *		

SUBPART J—ENHANCED PERSONNEL SECURITY PROGRAMS

110. Enhanced personnel security programs		11001
---	--	-------

Subpart A—General Provisions

* * * * *

Subpart J—Enhanced Personnel Security Programs

CHAPTER 110—ENHANCED PERSONNEL SECURITY PROGRAMS

<i>Sec.</i>	
11001. Enhanced personnel security programs	

(a) *DEFINITIONS.—In this section—*

(1) the term “agency” has the meaning given that term in section 3001 of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341);

(2) the term “consumer reporting agency” has the meaning given that term in section 603 of the Fair Credit Reporting Act (15 U.S.C. 1681a);

(3) the term “covered individual” means an individual who has been determined eligible for access to classified information or eligible to hold a sensitive position;

(4) the term “enhanced personnel security program” means a program implemented by an agency at the direction of the Director of National Intelligence under subsection (b); and

(5) the term “periodic reinvestigations” means investigations conducted periodically, with a frequency as required by the Director of National Intelligence, for the purpose of updating a previously completed security background investigation.

(b) **ENHANCED PERSONNEL SECURITY PROGRAM.**—The Director of National Intelligence shall direct each agency to implement a program to provide enhanced security review of covered individuals—

(1) in accordance with this section; and

(2) not later than the earlier of—

(A) the date that is 5 years after the date of enactment of the Enhanced Security Clearance Act of 2014; or

(B) the date on which the backlog of overdue periodic reinvestigations of covered individuals is eliminated, as determined by the Director of National Intelligence.

(c) **COMPREHENSIVENESS.**—

(1) **SOURCES OF INFORMATION.**—The enhanced personnel security program of an agency shall integrate relevant information from various sources, including government, publicly available, and commercial data sources, consumer reporting agencies, social media, and such other sources as determined by the Director of National Intelligence.

(2) **TYPES OF INFORMATION.**—Information obtained and integrated from sources described in paragraph (1) may include—

(A) information relating to any criminal or civil legal proceeding;

(B) financial information relating to the covered individual, including the credit worthiness of the covered individual;

(C) public information, including news articles or reports, that includes relevant security or counterintelligence information about the covered individual;

(D) publicly available electronic information, to include relevant security or counterintelligence information on any social media website or forum, that may suggest ill intent, vulnerability to blackmail, compulsive behavior, allegiance to another country, change in ideology, or any other information that may suggest the covered individual lacks good judgment, reliability or trustworthiness; and

(E) data maintained on any terrorist or criminal watch list maintained by any agency, State or local government, or international organization.

(d) **REVIEWS OF COVERED INDIVIDUALS.**—

(1) **REVIEWS.**—

(A) **IN GENERAL.**—The enhanced personnel security program of an agency shall require that, not less than 2 times every 5 years, the head of the agency shall conduct or re-

quest the conduct of automated record checks and checks of information from sources under subsection (c) to ensure the continued eligibility of each covered individual employed by the agency or a contractor of the agency, unless more frequent reviews of automated record checks and checks of information from sources under subsection (c) are conducted on the covered individual.

(B) *SCOPE OF REVIEWS.*—Except for a covered individual who is subject to more frequent reviews to ensure the continued eligibility of the covered individual, the reviews under subparagraph (A) shall consist of random or aperiodic checks of covered individuals, such that each covered individual is subject to at least 2 reviews during the 5-year period beginning on the date on which the agency implements the enhanced personnel security program of an agency, and during each 5-year period thereafter.

(C) *INDIVIDUAL REVIEWS.*—A review of the information relating to the continued eligibility of a covered individual under subparagraph (A) may not be conducted until after the end of the 120-day period beginning on the date the covered individual receives the notification required under paragraph (3).

(2) *RESULTS.*—The head of an agency shall take appropriate action if a review under paragraph (1) finds relevant information that may affect the continued eligibility of a covered individual.

(3) *INFORMATION FOR COVERED INDIVIDUALS.*—The head of an agency shall ensure that each covered individual employed by the agency or a contractor of the agency is adequately advised of the types of relevant security or counterintelligence information the covered individual is required to report to the head of the agency.

(4) *LIMITATION.*—Nothing in this subsection shall be construed to affect the authority of an agency to determine the appropriate weight to be given to information relating to a covered individual in evaluating the continued eligibility of the covered individual.

(5) *GUIDANCE FOR MINOR FINANCIAL OR MENTAL HEALTH ISSUES.*—The Director of National Intelligence shall issue guidance defining minor financial or mental health issues, in accordance with this section and any direction from the President.

(6) *AUTHORITY OF THE PRESIDENT.*—Nothing in this subsection shall be construed as limiting the authority of the President to direct or perpetuate periodic reinvestigations of a more comprehensive nature or to delegate the authority to direct or perpetuate such reinvestigations.

(e) *AUDIT.*—

(1) *IN GENERAL.*—Beginning 2 years after the date of implementation of the enhanced personnel security program of an agency under subsection (b), the Inspector General of the agency shall conduct at least 1 audit to assess the effectiveness and fairness, which shall be determined in accordance with performance measures and standards established by the Director of National Intelligence, to covered individuals of the enhanced personnel security program of the agency.

(2) SUBMISSIONS TO THE DNI.—The results of each audit conducted under paragraph (1) shall be submitted to the Director of National Intelligence to assess the effectiveness and fairness of the enhanced personnel security programs across the Federal Government.

