

UNCLASSIFIED//~~FOUO~~



FEB 03 2020

MEMORANDUM FOR: Distribution

SUBJECT: (U) Transforming Federal Personnel Vetting: Measures to Expedite Reform and Further Reduce the Federal Government's Background Investigation Inventory

- REFERENCES:
- A. (U) National Defense Authorization Act for Fiscal Year 2019, Public Law 115-232, Section 941 (codified at 50 U.S.C. § 3161 note) (U)
  - B. (U) Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, 18 Aug 2010 (U)
  - C. (U) Executive Order 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust, 16 Jan 2009 (as amended) (U)
  - D. (U) Executive Order 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, 2 Jul 2008 (as amended) (U)
  - E. (U) Homeland Security Presidential Directive-12, Policies for a Common Identification Standard for Federal Employees and Contractors, 27 Aug 2004 (U)
  - F. (U) Executive Order 12968, Access to Classified Information, 7 Aug 1995 (as amended) (U)
  - G. (U) Federal Investigative Standards, December 2012 (U//FOUO)
  - H. (U) Security Executive Agent Directive 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position, 12 Jun 2017 (U)
  - I. (U) Security Executive Agent Directive 4, National Security Adjudicative Guidelines, 8 Jun 2017 (U)
  - J. (U) Security Executive Agent Directive 7, Reciprocity of Background Investigations and National Security Adjudications, 9 Nov 2018 (U)

UNCLASSIFIED//~~FOUO~~

- K. (U) ODNI Memorandum ES 2017-00049, Strategy to Mitigate the Impact of National Background Investigations Bureau's Background Investigation Backlog, 16 Feb 17 (U//FOUO)
- L. (U) Joint ODNI and OPM Memorandum, Efficiencies for Background Investigations - Initiatives to Reduce Investigative Backlog and Mitigate Risk, 29 Nov 2017 (U//FOUO)
- M. (U) Joint ODNI and OPM Memorandum, Transforming Workforce Vetting, 2 May 2018 (U)
- N. (U) Joint ODNI and OPM Memorandum, Transforming Workforce Vetting: Measures to Reduce the Federal Government's Background Investigation Inventory in Fiscal Year 2018, 5 Jun 2018 (U//FOUO)

(U) During the past 18 months, members of the Trusted Workforce (TW) 2.0 Executive Steering Group have developed a new approach framework for Federal personnel vetting to ensure the Federal workforce is trusted to protect people, property, information, and mission (Reference N). The new approach framework has been approved by the Security Executive Agent and the Suitability & Credentialing Executive Agent.

(U) The TW 2.0 effort has led to the issuance of several mitigation measures outlined in References K, L, and N, as well as business process improvements implemented by the National Background Investigations Bureau (NBIB), now the Defense Counterintelligence and Security Agency (DCSA), and the Department of Defense (DoD). Implementation of these measures resulted in a significant reduction in the background investigation inventory from 725,000 to less than 214,000 as of January 27, 2020.

(U) This memorandum directs additional measures that will continue to reduce inventory. Some of these measures will also drive early adoption of important TW 2.0 reforms, such as the transition away from the traditional model of periodic reinvestigations to a future model that replaces periodic reinvestigations with government-wide continuous vetting of all populations (Reference D).

(U) This memorandum enables departments and agencies (D/As) to conduct continuous vetting for the national security population and cease conducting periodic reinvestigations (PR) for those personnel, as long as the D/As' continuous vetting programs satisfy the minimum standards set forth in Appendix 1. Additionally, this memorandum directs D/As to begin preparation for phased implementation of TW 2.0 reforms, such as Trusted Information Provider (TIP) programs.

- I. (U) **Additional Inventory Reduction Measures.** While the provisions in References K, L, and N remain effective—including authorization for agencies to defer PRs (Reference N, subparagraph I.1.(d))—additional measures have been identified to further reduce and

mitigate the background investigation inventory. Effective immediately, the following measures are available and apply to all authorized and delegated investigative agencies (i.e., Investigative Service Providers (ISP) and authorized adjudicative agencies):

1. (U) ***Compliance with PR Requirements through Continuous Vetting:***

(U) As described below, individuals investigated at Tiers 3 and 5, currently enrolled in a continuous vetting program that meets interim minimum standards set forth in Appendix 1, are deemed to be in compliance with PR requirements. This applies to populations enrolled in continuous vetting, including Federal civilian<sup>1</sup>, Federal contractor, military personnel, and state, local, tribal, and private sector personnel subject to Reference B.

- a. (U//~~FOUO~~) As long as the adjudicative record in the appropriate repository does not reflect information that calls one's eligibility into question, enrollment in a continuous vetting program, that meets standards in accordance with and as defined in Appendix 1, will be sufficient to meet the PR requirement. The Executive Agents (EA) require agencies to record continuous vetting enrollment in the government-wide repositories to reflect potential reciprocal eligibility.
- b. (U) This guidance will remain in effect at least until the final TW 2.0 policy is enacted, and existing Federal Investigative Standards (FIS) will be modified to reflect this policy change.
- c. (U) Agencies' continuous vetting programs are subject to EA oversight and audit. Agencies must be able to demonstrate effectiveness and compliance with the standards and implementation requirements set forth in Appendix 1.
- d. (U) (b)(3), (b)(7)(E) [REDACTED]
- e. (U) (b)(3), (b)(7)(E) [REDACTED]
- f. (U) The EAs will propose rulemaking to support these measures.

---

<sup>1</sup> (U) The EAs have determined that continuous vetting at Tier 3 and 5 is consistent with the requirement for 'reinvestigation' of every covered employee occupying a position of public trust.

2. (U) *Clarifications and Revisions to the Existing Federal Investigative Standards:*

- a. (U//~~FOUO~~) ISPs will close and deliver, to the responsible adjudicative entity, all Tier 1-5 initial and reinvestigation cases that meet the FIS modified by the criteria outlined in subparagraphs 2.b.i-v, below.
- b. (U//~~FOUO~~) All D/As will also consider these cases complete and will not request additional investigative coverage. However, the provisions of paragraph 11.2.5 of the FIS (additional investigation to resolve issues to render an adjudicative determination) are still applicable. To ensure reciprocity, D/As should not apply exception codes to these adjudications when reporting to the government-wide adjudication and clearance repositories. If favorably adjudicated, these investigations are to be reciprocally accepted by all D/As.

i. (U//~~FOUO~~) Selective Service Checks for all Tiers:

(U//~~FOUO~~) ISPs are no longer required to conduct a check of the Selective Service database for a record of registration and ISPs will close cases without verifying Selective Service registration record.

ii. (U//~~FOUO~~) Internal Revenue Service Tax Compliance Checks:

(U//~~FOUO~~) (b)(3), (b)(7)(E)

[REDACTED]

iii. (U//~~FOUO~~) (b)(3), (b)(7)(E)

(U//~~FOUO~~) (b)(3), (b)(7)(E)

[REDACTED]

(U//~~FOUO~~) (b)(3), (b)(7)(E)

[REDACTED]

(U//~~FOUO~~) (b)(3), (b)(7)(E)

[REDACTED]



(b)(3), (b)(7)(E)

iv. (U//~~FOUO~~) (b)(3), (b)(7)(E)

(U//~~FOUO~~) (b)(3), (b)(7)(E)

v. (U//~~FOUO~~) Investigative Methods for Collection of Information from an Individual:

(U//~~FOUO~~) ISPs are permitted to leverage the spectrum of investigative methods available to meet an investigation's coverage requirements or to address a specific issue at any time during the investigative process. This approach provides the ISP with a degree of flexibility when determining the most cost-effective methods while balancing risks and benefits to satisfy requirements while ensuring uniformity to support reciprocal recognition of investigations. These alternative methods may include an electronic interview capability, telephonic contact, a video teleconference interview or other non-traditional methods to collect additional information from the individual, resolve discrepancies, or conduct reference or social interviews (listed or developed). Refer to previously issued Reference L for details on these methods. Prior to leveraging additional methods not already approved, an ISP must obtain written approval from the EAs. ISPs must carefully document alternative collection methodologies in support of oversight.

3. (U) *Use of Annual Vetting Appraisals:*

(U) When fully developed and implemented, continuous vetting may include a process for D/As to annually appraise individuals' background and identify individuals who may require additional support or assistance to prevent behavior from presenting a serious, future concern. Any D/As developing this, or a similar capability, are required to consult with and obtain written approval from the EAs prior to conducting a pilot or similar assessment and prior to its implementation. All information obtained via such an annual appraisal shall be handled in accordance with applicable law and policy, including the Privacy Act of 1974, and forthcoming EA guidance.

4. (U) *Trusted Information Provider Program:*

(U) New Trusted Information Provider (TIP) guidelines and standards are under development and will be coordinated as part of the TW 2.0 policy framework. To inform policy development, ISPs, D/As, industry, and the military services will work with the EAs to inform aspects of implementing the TIP program. ISPs will be subject to EA oversight, including due diligence to comply with applicable law, and

must comply with requirements prescribed by the EAs pursuant to forthcoming EA guidance.

**II. (U) Measures Related to TW 2.0 Implementation.** Consistent with their responsibilities, pursuant to Section 2.7(b) of Reference D, and pursuant to forthcoming guidance, heads of agencies shall prepare for the following:

1. (U) *Expedited Policy Coordination:*

(U) D/As are to ensure that policy and operational personnel participate in the interagency process for developing and vetting the new TW 2.0 policy framework as it goes through coordination as well as facilitate expedited agency review and comment on the upcoming policy issuances.

2. (U) *Transition from PRs to Continuous Vetting:*

- a. (U) As we begin the process of replacing traditional PRs with continuous vetting, starting with the Tier 3 and Tier 5 population (see Appendix 1), all D/As will take the necessary steps to prepare their workforce for the government-wide transition to continuous vetting. This includes, among other matters, budgeting, personnel, policy, process, information technology (IT) changes, and compliance with all applicable law (e.g., amending any system of records notices).

- b. (U) D/As are reminded that they still must comply with the Security EA 2020 Continuous Evaluation (CE) implementation requirement, to conduct automated CE checks of all required data sources at the required periodicities (b)(3), (b)(7)(E) [REDACTED] Refer to Appendix 1 for further information regarding how CE sources relate to the Continuous Vetting Standards.

3. (U) (b)(3), (b)(7)(E) [REDACTED]

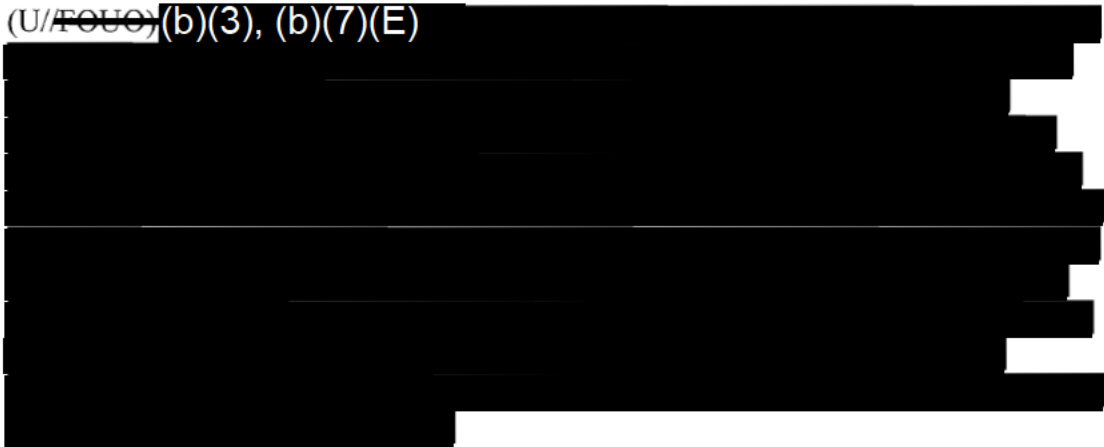
(U//~~FOUO~~) (b)(3), (b)(7)(E) [REDACTED]

4. (U) *Opportunities to Gain Efficiencies:*

(U) D/As will work with the EAs to begin streamlining their agency personnel vetting programs in anticipation of upcoming policy changes to better align processes and criteria used for vetting determinations to eliminate unnecessary duplicative applications, investigations, adjudications, and access determinations.

5. (U) *State, Local, and Tribal Law Enforcement Criminal History Record Information:*

(U//~~FOUO~~)(b)(3), (b)(7)(E)

A large rectangular area of the document is completely redacted with black ink, covering approximately five lines of text.


6. (U) *Credentialing Standards:*

(U) When the Suitability and Credentialing Executive Agent finalizes new government-wide credentialing standards, guidelines, and procedures for issuing, suspending, or revoking eligibility for HSPD-12 Personal Identity Verification credentials to employees and contractor personnel, D/As will align their other vetting processes with the government-wide credentialing standards, guidelines, and procedures.

III. (U) **Continuing Applicability of Previous Executive Agent Guidance:** D/As are reminded of the continued applicability of the following backlog mitigation actions (References K and N) where an individual does not meet the criteria in paragraph I.1.

1. (U) *Background Investigation Validity and Reciprocity:*

(U//~~FOUO~~)(b)(3), (b)(7)(E)

A large rectangular area of the document is completely redacted with black ink, covering approximately six lines of text.

UNCLASSIFIED//~~FOUO~~

2. (U) *Deferral of Reinvestigations:*

(U//~~FOUO~~) (b)(3), (b)(7)(E)

[REDACTED]

3. (U) *Acceptance of Active National Security Determinations by Other Agencies:*

(U//~~FOUO~~) (b)(3), (b)(7)(E)

[REDACTED]

(U) These measures, taken together with those outlined in References K, L, and N, are part of a comprehensive strategy to continue to reduce the background investigation inventory, increase investigative resources and production, incorporate business transformation efficiencies, and streamline quality review processes. The EAs are committed to working with the PAC and key stakeholders to further the TW 2.0 efforts to transform the Federal personnel vetting mission.

(U) This memorandum is effective until revoked in writing. Questions regarding national security determinations should be directed by email to SecEA@dni.gov. Questions pertaining to suitability and fitness determinations should be directed by email to SuitEA@opm.gov, and questions pertaining to credentialing determinations should be directed by email to CredEA@opm.gov.



Joseph Maguire  
Acting Director of National Intelligence  
Security Executive Agent



Dale Cabaniss  
Director, Office of Personnel Management  
Suitability and Credentialing Executive Agent

Attachments:

1. (U) Appendix 1, Interim Minimum Standards for Continuous Vetting
2. (U) Template for Agency Memorandum, Continuous Vetting Worksheet, and Instructions

UNCLASSIFIED//~~FOUO~~



Distribution:

Secretary of State  
Secretary of the Treasury  
Secretary of Defense  
Attorney General  
Secretary of the Interior  
Secretary of Agriculture  
Secretary of Commerce  
Secretary of Labor  
Secretary of Health and Human Services  
Secretary of Housing and Urban Development  
Secretary of Transportation  
Secretary of Energy  
Secretary of Education  
Secretary of Veterans Affairs  
Secretary of Homeland Security  
Administrator, Environmental Protection Agency  
Director, Office of Management and Budget  
United States Trade Representative  
Administrator, Small Business Administration  
Director, Central Intelligence Agency  
Director, Office of National Drug Control Policy  
Secretary of the Army  
Secretary of the Navy  
Secretary of the Air Force  
Chairman, Joint Chiefs of Staff  
Chairman of the Board of Governors, Federal Reserve Board  
Commissioner, Social Security Administration  
Director, National Science Foundation  
Administrator, National Aeronautics and Space Administration  
Administrator, United States Agency for International Development  
Commissioner, Nuclear Regulatory Commission  
Director, Office of Personnel Management  
Under Secretary for Intelligence, Department of Defense  
Under Secretary for Intelligence and Analysis, Department of Homeland Security  
Director, Federal Bureau of Investigation  
Director, United States Secret Service  
Director, National Security Agency  
Director, Defense Advanced Research Projects Activity  
Director, Defense Information Systems Agency  
Director, National Reconnaissance Office  
Director, Defense Intelligence Agency  
Director, Defense Logistics Agency  
Director, Defense Contract Audit Agency  
(Continued)

Director, Defense Counterintelligence and Security Agency  
Director, Defense Finance and Accounting Services  
Director, National Geospatial-Intelligence Agency  
Director, Missile Defense Agency  
Director, Bureau of Alcohol, Tobacco, Firearms and Explosives  
Director, Office of Science and Technology Policy  
Director, Executive Office of the President, Office of Administration  
Commandant, United States Marine Corps  
Commissioner, United States Customs and Border Protection  
Administrator, Drug Enforcement Administration  
Chief, National Guard Bureau  
Chairman, Federal Trade Commission  
Chairman, International Trade Commission  
Chairman, Securities and Exchange Commission  
Archivist, National Archives and Records Administration  
Chairman, Federal Communications Commission  
Chairman, National Labor Relations Board  
Administrator, General Services Administration  
Director, United States Peace Corps  
Chairman, Federal Maritime Commission  
Administrator, Equal Employment Opportunity Commission  
Director, Office of Government Ethics  
Postmaster General, United States Postal Service  
Director, Selective Service System  
Director, Broadcasting Board of Governors  
Assistant Secretary, Bureau of Intelligence and Research, Department of State  
Assistant Secretary, Intelligence and Analysis, Department of Treasury  
Inspector General, Department of Defense  
Director, Office of Intelligence and Counterintelligence, Department of Energy  
Director of Naval Intelligence, United States Navy  
Director of Intelligence, Headquarters, United States Marine Corps  
Deputy Chief of Staff, Headquarters, United States Army  
Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance, United States Air Force  
Assistant Commandant for Intelligence and Criminal Investigations, United States Coast Guard  
Director, Information Security Oversight Office  
Executive Assistant Director, Intelligence Branch, Federal Bureau of Investigation  
Chief of Intelligence/Senior Officer, Drug Enforcement Administration  
Chief Postal Inspector, United States Postal Inspection Service

## **(U) Appendix 1: Interim Minimum Standards for Continuous Vetting**

### **I. (U) Purpose**

(U//~~FOUO~~) This Appendix contains interim minimum standards for continuous vetting for all personnel who have been investigated at Tier 3 or Tier 5 to ensure consistent application and to promote reciprocal acceptance for vetting determinations across the Executive Branch. Compliance with these continuous vetting minimum standards will establish an interim milestone for transitioning from the current periodic reinvestigation-based construct to the TW 2.0 framework for Executive Branch-wide continuous vetting. This document supplements any prior authority to conduct continuous vetting, including EA memoranda authorizing use of continuous vetting procedures to reduce the investigative backlog. These standards remain in effect until they are further defined by the EAs for the TW 2.0 effort.

### **II. (U) Background**

(U//~~FOUO~~) Traditionally, the Federal government has vetted individuals for trustworthiness with an initial background investigation and subsequent periodic reinvestigations. The current FIS, issued in 2012, introduced continuous evaluation as a supplement to PRs for positions with the highest levels of risk. In 2018, SEAD 6, Continuous Evaluation, provided further clarification.

(U) In 2017, EO 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information was amended to include the new concept of continuous vetting, and mandated continuous vetting for all populations, not just those at the highest levels of risk. In accordance with Security, Suitability, and Credentialing Executive Agents Correspondence, Transforming Workforce Vetting: Measures to Reduce the Federal Government's Background Investigation Inventory in Fiscal Year 2018, the EAs authorized agencies to defer some periodic reinvestigations if the individual could be enrolled in continuous vetting.

(U) Continuous vetting is the evolution of the continuous evaluation concept. CE data sources, originally intended to supplement periods between reinvestigations, have become a fundamental basis for continuous vetting. A fully compliant continuous vetting program includes the required CE data sources as well as agency-specific data sources, such as user activity monitoring where appropriate, that permit agencies, when fully compliant, to cease conducting periodic reinvestigations.

### **III. (U) Applicability**

(U) These standards apply to any individual (including Federal civilian, Federal contractor, military personnel, and state, local, tribal, and private sector personnel subject to EO 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities) who is enrolled in a continuous vetting program that satisfies Tier 3 and Tier 5 periodic reinvestigation requirements and meets the requirements of this Appendix. These standards do not apply to other tiers.



#### IV. (U) Minimum Standards

(U) Continuous vetting is defined in EO 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information as “reviewing the background of a covered individual at any time to determine whether that individual continues to meet applicable requirements.” To be compliant with these minimum standards, D/A continuous vetting programs must be certified to the Security and Suitability/Credentialing Executive Agents with written submission of the attached memorandum and worksheet indicating that all requirements are being met to SecEA@dni.gov and SuitEA@opm.gov.

- (U) D/As with investigative authority may develop their own continuous vetting capabilities in accordance with these minimum standards. However, D/As are encouraged to use continuous vetting capabilities offered as a shared service by authorized investigative agencies.
  - (U) D/As that do not obtain continuous vetting capabilities from authorized investigative agencies, and which do not have their own investigative authority must continue conducting PRs for their populations.
  - (U) D/As shall coordinate continuous vetting activities internally with appropriate stakeholders such as their offices of the chief information officer, chief security officer, human resources, general counsel, chief privacy officer, insider threat manager, counterintelligence, and component organizations to manage programs and capabilities. These offices should regularly coordinate to ensure that the conduct of continuous vetting is being managed in a manner that meets the standards set forth herein.
  - (U) D/As must clearly delineate roles and responsibilities of agency personnel security, human resources, insider threat personnel, information security, facility security, inspector general, and other appropriate personnel involved in continuous vetting programs. This includes but is not limited to designating entities or individuals responsible for collecting and maintaining information, coordinating between entities, reporting and maintaining information in the appropriate system or record or repository, managing alerts, resolving issues, and handling subsequent actions.
  - (U) D/As must adhere to notice and redress requirements associated with an unfavorable determination.
1. (U) Data Checks. Except for individual interviews, all of the following data checks, to be conducted by authorized ISPs, are required at a minimum and at no less than the periodicity specified:



Table 1 - (U//FOUO) Continuous Vetting Required Checks for TW 2.0

CE Required Checks	Data Sources	Minimum Periodicity
Eligibility	(b)(3), (b)(7)(E)	(b)(3), (b)(7)(E)
Terrorism	(b)(3), (b)(7)(E)	(b)(3), (b)(7)(E)
Criminal Activity	(b)(3), (b)(7)(E)	(b)(3), (b)(7)(E)
Foreign Travel	(b)(3), (b)(7)(E)	(b)(3), (b)(7)(E)
Suspicious Financial Activity	(b)(3), (b)(7)(E)	(b)(3), (b)(7)(E)
Credit Bureau Checks	(b)(3), (b)(7)(E)	(b)(3), (b)(7)(E)
Public Record Checks (judgments, liens, bankruptcies, etc.)	(b)(3), (b)(7)(E)	(b)(3), (b)(7)(E)
Additional Required Checks		
Employment Conduct	(b)(3), (b)(7)(E)	(b)(3), (b)(7)(E)
Criminal Activity	(b)(3), (b)(7)(E)	(b)(3), (b)(7)(E)
Permitted but Not Required		
Individual Interviews	(b)(3), (b)(7)(E)	(b)(3), (b)(7)(E)

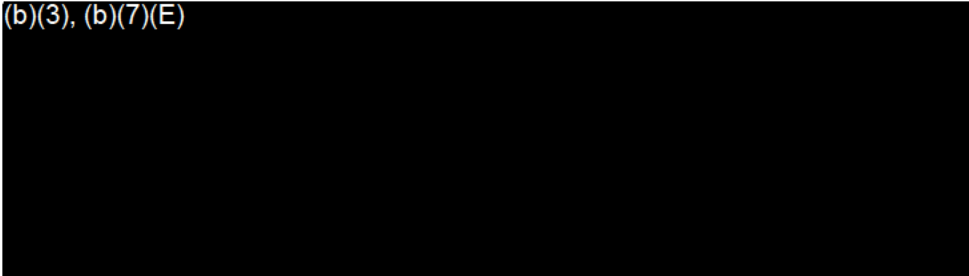
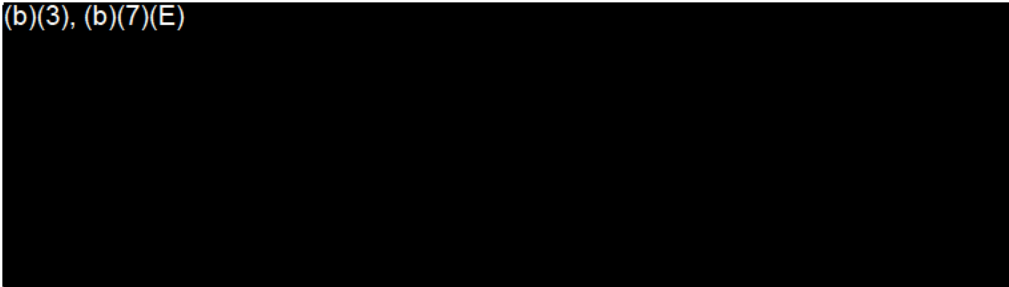
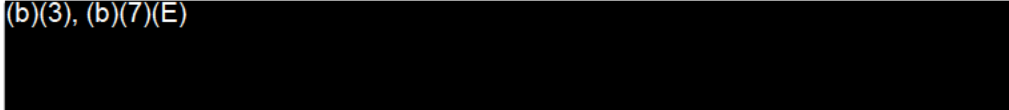
(U) Table is Unclassified//~~FOUO~~ Official Use Only

\*(U//~~FOUO~~) ISPs with existing capability to conduct (b)(3), (b)(7)(E)

2. (U) Agency-specific Information

- a. (U//~~FOUO~~) D/As must incorporate into their ISP's continuous vetting process adjudicative relevant information obtained from the following agency-specific data sources:
  - i. (U//~~FOUO~~) Insider threat-related information;
  - ii. (U//~~FOUO~~) Security incidents/violations;
  - iii. (U//~~FOUO~~) User activity monitoring;
  - iv. (U//~~FOUO~~) Internal misconduct investigations and disciplinary actions taken;
  - v. (U//~~FOUO~~) Self-reported information; and
  - vi. (U//~~FOUO~~) Third-party reported information.
- b. (U) D/As may augment the automated data checks and required agency-specific data with collection of additional adjudicatively relevant information from other agency-specific sources, as available, to reduce the risk to people, property, information, and mission.

3. (U) Alert Management and Issue Resolution

- a. (b)(3), (b)(7)(E)  

- b. (U) D/As also must develop processes to ensure that identified issues of concern are evaluated in a timely manner, once known, to determine the effect on an individual's continued eligibility and access.
- c. (b)(3), (b)(7)(E)  

- d. (b)(3), (b)(7)(E)  


(b)(3), (b)(7)(E)

- c. (U//~~FOUO~~) Reporting. D/As are responsible for updating the government-wide repositories with the accurate enrollment status of those individuals in continuous vetting as well as any change in eligibility resulting from continuous vetting alerts. D/As are also responsible for ensuring that information developed as part of continuous vetting or issue resolution, including internal agency information discussed in section 4(a) and (b), is accurate and incorporated into an individual's investigative record.

## V. (U) D/A Responsibilities

1. (U) Required Reporting to EAs. D/As are required to submit the following to the EAs:
  - a. (U) Before using continuous vetting to satisfy PR requirements, a D/A must submit a memorandum—example below—to the EAs with the attached worksheet (below) demonstrating compliance with the requirements of continuous vetting to satisfy PR requirements.
  - b. (U) Upon request of the EA(s), for oversight purposes, D/As must provide the following:
    - i. (U) Documentation of the continuous vetting program, capabilities, data categories and sources;
    - ii. (U) Protocols and processes for addressing validated alerts and prioritization;
    - iii. (U) Investigative products provided by the ISP, as well as internal/external agencies sources used to achieve the minimum vetting requirements; and
    - iv. (U) Processes for access to, managing, and protecting sensitive or private information.
  - c. (U) The following metrics will be added to the ODNI reporting requirements and included in the quarterly submissions:
    - i. (U//~~FOUO~~) The agency's number of individuals enrolled in a continuous vetting program by investigative tier (Tier 3 or 5);
    - ii. (U//~~FOUO~~) Total number of PR deferrals for both Tier 3 and Tier 5;
    - iii. (U//~~FOUO~~) Total number of PR submissions for both Tier 3 and Tier 5; and
    - iv. (U//~~FOUO~~) Count and average age of continuous vetting alerts that are "Not Yet Resolved" (See resolution status (a), as defined below).

2. (U) Using an appropriate forum, D/As using continuous vetting programs are expected to share best practices and identify potential continuous vetting refinements.

## VI. (U) Definitions

1. (U) Resolution Status. The resolution status of an alert is defined, as follows:
  - a. (U) **Not Yet Resolved** – The alert is still open and no resolution status has been defined.
  - b. (U) **Closed, No Action Taken** – The alert has been evaluated to determine the impact on an individual's eligibility and it was determined that no action was required at this time.
  - c. (U) **Closed, Exception Assigned** – The alert has been evaluated to determine the impact on an individual's eligibility and it was determined that a condition or waiver should be added to an individual's eligibility.
  - d. (U) **Closed, Eligibility Suspended or Revoked** – The alert has been evaluated to determine the impact on an individual's eligibility and it was determined that the individual's eligibility should be suspended or revoked.



**AGENCY LETTERHEAD**

MEMORANDUM FOR: Director of National Intelligence  
Security Executive Agent

Director, Office of Personnel Management  
Suitability and Credentialing Executive Agent

SUBJECT: (U) Compliance with Continuous Vetting to Satisfy Periodic  
Reinvestigation Requirements for National Security and Sensitive  
Positions at Tiers 3 and 5

REFERENCE: (U) ODNI-OPM Memorandum, Transforming Federal Personnel  
Vetting: Measures to Expedite Reform and Further Reduce the  
Federal Government's Background Investigation Inventory,  
3 Feb 2020

(U) (AGENCY) hereby certifies to the Executive Agents its ability to conduct compliant Continuous Vetting for National Security Investigations for personnel meeting the definition as stated in the reference, Section I (1). (AGENCY) shall comply with all Security Executive Agent Directives, Correspondence and Standards that affect National Security Investigations for positions designated as National Security or Sensitive.

(U) As proof of compliance with data source and agency-specific information requirements, the agency attaches the Continuous Vetting Worksheet as required by the reference, Appendix 1.

(U) (AGENCY) further acknowledges the quarterly reporting requirements found in the reference, Appendix 1.

(U) (AGENCY) also certifies compliance with the Alert Management and Issue Resolution requirements of the reference, Appendix 1.

(U) (AGENCY) acknowledges that upon request of the Executive Agent(s), for oversight purposes, (AGENCY) must provide documentation as specified in Section V.1.(b) of the reference.

(U) For questions or concerns, please contact (AGENCY Point of Contact) at (Phone Number or email).

\_\_\_\_\_  
Head of Agency name and title

\_\_\_\_\_  
Date

Attachment: (U) Continuous Vetting Worksheet

Attachment: (U) Continuous Vetting Worksheet  
(U) Continuous Vetting Worksheet Table 2- (U//FOUO) CV Certification

This Table is Unclassified//For Official Use Only

Department and or Agency			
Date Worksheet Completed			
Continuous Vetting Plans must be compliant with the below checks			
1	Eligibility	(b)(3), (b)(7)(E)	Yes Provider Name
2	Terrorism	(b)(3), (b)(7)(E)	Yes Provider Name
3	Criminal	(b)(3), (b)(7)(E)	Yes Provider Name
4	Foreign Travel	(b)(3), (b)(7)(E)	Yes Provider Name
5	Suspicious Financial	(b)(3), (b)(7)(E)	Yes Provider Name
6	Credit Bureau	(b)(3), (b)(7)(E)	Yes Provider Name
7	Public Records	(b)(3), (b)(7)(E)	Yes Provider Name
8	Employment	(b)(3), (b)(7)(E)	Yes Provider Name
9	Agency Specific Information		Yes Provider Name
		Insider Threat	
		Security Incidents/Violations	
		UAM	
		Internal Investigations	
		Interview of Individual	
		Self Report	
	3rd Party Reporting		
10	Criminal Activity	(b)(3), (b)(7)(E)	Yes Provider Name

This Table is Unclassified//~~For Official Use Only~~

**(U) Continuous Vetting Worksheet Instructions**

**(U) Department/Agency:** Provide the name of the Department, Agency, and/or component, or any subsidiaries thereof that are to be included in the certification form.

**(U) Date Completed:** The date that certification form was completed.

**(U) Yes/Name of Investigative Service Provider (ISP):** Indicate in the block with a check mark that the listed check is being completed as required and identify the ISP performing such check in the provider name section.