Federal Personnel Vetting Performance Management Standards

I.   Purpose

This document and corresponding appendices constitute the minimum standards for the ongoing assessment of Federal personnel vetting policies and business processes in order to enable effective, data-driven decision-making by policymakers, department and agency (D/A) heads, and program managers. Assessments are informed by robust performance management practices that measure efficiency, effectiveness, fairness, and risk across the Federal personnel vetting enterprise.

The subordinate appendices identify performance management standards that will be used by the Security, Suitability, and Credentialing Executive Agents (EA) and Executive Branch entities engaging in Federal personnel vetting performance management activities to assess the success of personnel vetting programs and policies. Specifically, Appendix A identifies minimum performance metrics, and Appendix B sets forth requirements for quality management programs. In performance of their oversight responsibilities or to meet reporting obligations, the EAs may, collectively or individually, request additional performance metrics from the D/As, authorized personnel vetting investigative service providers (ISP), authorized adjudicative entities, and shared service providers.

II.   Authorities

These Standards are issued by the EAs[1] pursuant to the following authorities:

  A. 5 U.S.C. 1103, 1104, 3301, 3302, and 11001;

  B. 50 U.S.C. 3024, 3161, 3162a, 3341;

  C. 5 C.F.R. parts 2, 5, 6, 731, and 1400;

  D. E.O. 12968, Access to Classified Information (02 August 1995), as amended;

  E. E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information (30 June 2008), as amended;

---

[1] Pursuant to Executive Order (E.O.) 13467, as amended, the Director of the Office of Personnel Management is the Suitability and Credentialing Executive Agent and, per section 803 of the National Security Act and Executive Order 13467, as amended, the Director of National Intelligence is the Security Executive Agent.

F. E.O. 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust (16 January 2009), as amended; and

G. Homeland Security Presidential Directive 12, Policies for a Common Identification Standard for Federal Employees and Contractors (27 August 2004).

III. Scope, Applicability, and Review

A. These Standards are consistent with the *Federal Personnel Vetting Core Doctrine* and the *Federal Personnel Vetting Guidelines* that establish desired outcomes for successful personnel vetting programs, and the *Performance Management Guidelines* that describe the desired performance management outcomes when evaluating the efficiency, effectiveness, fairness, and risk of Federal personnel vetting programs.

B. These Standards apply, to the extent permitted by law, to Executive Branch entities engaging in Federal personnel vetting performance management activities, including:

1. D/A personnel vetting program management offices and suitability, fitness, national security, and credentialing programs;

2. ISPs;

3. Authorized adjudicative entities; and

4. Executive Branch shared service providers.

C. These Standards outline the minimum performance metrics and measures needed to assess the success of the personnel vetting programs and empower stakeholders to make decisions, improve processes, and assign accountability.

D. In applying these Standards, D/As must protect the privacy and civil liberties of all individuals in accordance with the Privacy Act and other applicable laws, regulations, and policies and make sure there is consistent treatment, equity, and fairness when implementing these standards in the personnel vetting process.

E. Internal D/A policies must comply with these Standards absent D/A-specific obligations pursuant to statute or E.O., or Executive Agents' approval of a waiver or exceptions.

F. The EAs, or their designees, will review these Standards, including the appendices listed in the table below, and revise them as necessary to respond to evolving threats, societal trends, changes to law or policy, or research and innovation, or to accommodate process or technology improvements. At a minimum, the EAs, or their designees, will review these Standards every five years to ensure the Standards maintain a high level of efficiency, effectiveness, and fairness within Federal personnel vetting programs.

Appendix	Description
Appendix A	Performance Metrics
Appendix B	Quality Management Programs

G. These Standards remain in effect until revoked in writing by the EAs.

IV.   Personnel Vetting Performance Management Principles

The personnel vetting performance management principles listed below must be applied at the enterprise, D/A, and personnel vetting program levels, and will guide practitioners, policymakers, and leadership in improving the efficiency, effectiveness, and fairness of Federal vetting programs while also managing risk in this area.

A. Minimize the time it takes to convert an outsider into a trusted insider and put the individual to work supporting the mission.

B. Improve the mobility of the Federal workforce (including contractors) for all vetting scenarios.

C. Maximize efficiency, effectiveness, fairness, and quality of the Federal personnel vetting enterprise.

D. Manage risk across the five personnel vetting scenarios.

E. Leverage information technology shared services and emerging technologies, as appropriate.

F. Share information, as appropriate.

V.   Policy and Responsibilities

Personnel vetting performance management encompasses the processes to collect, analyze, and report information about personnel vetting performance, and to use that information to continually manage risk and improve the effectiveness, efficiency, and fairness of personnel vetting operations across all five personnel vetting scenarios and each personnel vetting domain (suitability, fitness, national security, and credentialing).

Performance metrics (or data) collected from D/As, shared service providers, ISPs, and authorized adjudicative entities will be used in oversight performance and quality assessment programs.

A. The EAs will:

1. Provide implementation guidance that addresses relevant performance goals, performance metrics, and reporting schedules, and regularly evaluate and update such guidance as necessary;

2. Collect the minimum performance metrics data identified in Appendix A in accordance with the reporting schedule established in the implementation guidance;

3. Retain the authority to collect additional performance metrics pursuant to Congressional or other requirements;

4. Identify automated IT capabilities on classified and unclassified systems to streamline the reporting of performance metrics to the greatest extent

practicable, and make such capabilities available for integration by D/As, shared service providers, ISPs, and authorized adjudicative entities;

5. Assess whether the reported performance metrics data meet established requirements, analyze the metrics data to identify opportunities for systemic improvements, enterprise-wide innovation, and policy enhancements, and monitor actions taken across the enterprise to continuously improve personnel vetting performance; and

6. Report enterprise performance to appropriate entities in order to comply with statutory reporting requirements and support transparency.

B. D/As will each:

1. Account for these Standards in the collection of performance metrics data, the development of quality assessments, and efforts to continuously improve processes, where applicable, to effectively manage its personnel vetting program;

2. Collect personnel vetting performance metrics, such as data related to costs, personnel, volumes, times, and levels of effort in accordance with law, regulation, and policy. D/As will be responsible for collecting (preferably electronically) its own metrics and ensuring that the high and low side government-wide repositories have the required data to enable analysis and reporting of enterprise-wide metrics. D/As may leverage ISPs, authorized adjudicative entities, and shared service providers to collect personnel vetting performance metrics;

3. Analyze performance data by identifying how it meets desired outcomes and performance goals. If a gap is identified between the observed performance metrics and the desired outcome, the D/A must identify corrective actions to continuously improve personnel vetting and mitigate the performance gap;

4. Report performance metrics data to EAs in accordance with the reporting schedule established in the implementation guidance;

5. Propose new performance metrics to the EAs that could help improve decision-making and identify existing performance metrics that are not providing value at the D/A;

6. Monitor and evaluate the effectiveness of actions taken to improve the vetting process at the D/A;

7. Collaborate with complementary mission partners to align performance metrics data collection and prevent gaps in accountability of the personnel vetting process;

8. Integrate emerging technology, research findings, innovations, and EA-approved automated capabilities to the greatest extent possible to improve personnel vetting performance management and streamline the reporting of performance metrics data;

9. Assess whether to develop its own performance metrics in addition to the ones listed in these Standards. Each D/A may develop and implement its own performance metrics and is not limited in the frequency of its performance metrics collection; and

10. Ensure personnel responsible for personnel vetting performance management (personnel vetting practitioners, quality control managers, etc.) have completed appropriate training related to awareness of unconscious bias and ethnic and cultural differences among people to allow them to effectively identify case-specific and systems problems.

C. ISPs, authorized adjudicative entities, and shared service providers, will each:

1. Incorporate performance management to effectively manage its personnel vetting programs;

2. Collect required performance metrics data on behalf of its D/A customers;

3. Analyze its performance by identifying how it meets desired outcomes and performance goals. If a gap is identified between the observed performance metrics and the desired outcome, the ISP, authorized adjudicative entity, or shared service provider must identify corrective actions to continuously improve personnel vetting and mitigate the performance gap;

4. Report performance metrics data to the EAs, high and low-side government-wide repositories, as applicable, and to appropriate customer D/A(s) in accordance with the reporting schedule established in the implementation guidance;

5. Propose new performance metrics to the EAs that could help improve decision-making and identify existing performance metrics that are not providing value at the shared service provider-level;

6. Monitor and evaluate the effectiveness of actions taken to improve the vetting process;

7. Collaborate with complementary mission partners to align performance metrics data collection and prevent gaps in accountability of the personnel vetting process;

8. Integrate emerging technology, research findings, innovations, and EA-approved automated capabilities to improve personnel vetting performance management and streamline the reporting of performance metrics data, to the greatest extent possible;

9. Assess whether to develop its own performance metrics in addition to the ones listed in these Standards. Each ISP, authorized adjudicative entity, and shared service provider may develop and implement its own performance metrics and is not limited in the frequency of its data collection; and

10. Ensure personnel responsible for personnel vetting performance management (personnel vetting practitioners, quality control managers, etc.) have

completed appropriate training related to awareness of unconscious bias and ethnic and cultural differences among people to allow them to effectively identify case-specific and systems problems.

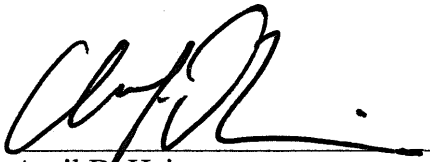## VI. Personnel Vetting Performance Management Metrics

The three major performance management components are the Performance Measurement Framework, Information Collection Framework, and Analysis and Reporting Framework, as described in the *Federal Personnel Vetting Performance Management Guidelines*. By implementing these components, D/As, ISPs, authorized adjudicative entities, and shared service providers will assist the EAs, the Security, Suitability, and Credentialing Performance Accountability Council (PAC), and other stakeholders with continuous process improvement across each personnel vetting domain.

Outcome-based performance metrics support data-driven, transparent policy-making processes, as well as identify and drive enterprise-level process enhancements to ensure improved risk mitigation, customer service, and appropriate consideration of stakeholder equities.
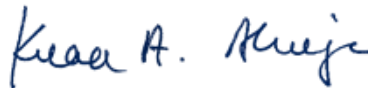
As reflected in Appendix A, performance metrics should be collected according to entity, category, and type:

A. Entities: "Entities" represent the collection of performance metrics from specific sectors within the vetting enterprise. Entities include:

    1. D/A;

    2. ISP;

    3. Authorized adjudicative entity; and

    4. Shared service provider.

B. Categories: "Categories" represent performance metrics that provide meaningful performance information to stakeholders to enable recognition of risks, issues, and trends, and to help identify causes in order to implement tailored mitigation strategies. Each performance metric is assigned one of the following performance categories:

    1. Health—Aggregated performance metrics that provide indications of the complexity, productivity, and proficiency of vetting programs and activities.

    2. Reform—Performance metrics used to drive implementation, policy decisions, and development of enterprise-wide reforms. Reform performance metrics may also measure the implementation and full operating capabilities of emerging reform initiatives or new policy/legislative mandates.

    3. Special Interest—Performance metrics used to inform policy decisions and program development related to evolving threats, societal trends, research and innovation, or to accommodate process or technology improvements.

C. Types: Each performance metric is assigned one or more of the following performance metric types:

1. Efficiency—Performance metrics that reflect whether an activity is being performed in the best possible manner with minimal waste of resources, to include time, cost, personnel, budgets, volumes, and effort. These metrics support the five personnel vetting scenarios.

2. Effectiveness—Performance metrics that reflect whether an activity is achieving the intended result and whether the activity is aligned with intent of Federal personnel vetting policy. These metrics support achieving quality and desired outcomes.

3. Risk—Performance metrics that indicate when processes are prone to vulnerabilities and threats, to include system availability and systemic risk to the success of the Federal personnel vetting enterprise. This includes performance metrics that may indicate fairness and whether processes and decisions are consistent across all cases and situations of the same type and in accordance with applicable laws, regulation, and policy.

Avril D. Haines
Director of National Intelligence
Security Executive Agent

Kiran A. Ahuja
Director
Office of Personnel Management
Suitability and Credentialing Executive
Agent

September 13, 2022
Date

September 14, 2022
Date

Enclosures:
1. Performance Management Standards, Appendix A: Performance Metrics (U)
2. Performance Management Standards, Appendix B: Quality Management Programs (U)

7

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, Office of Science and Technology Policy
Director, Office of Administration, Executive Office of the President
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 of the Federal Reserve
Commissioner, Social Security Administration
Director, Central Intelligence Agency
Director, National Science Foundation
Administrator, National Aeronautics and Space Administration
Administrator, United States Agency for International Development
Commissioner, Nuclear Regulatory Commission
Under Secretary for Intelligence and Security, Department of Defense
Under Secretary for Intelligence and Analysis, Department of Homeland Security
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 Logistics Agency
Director, Defense Intelligence Agency
Director, Defense Contract Audit Agency
Director, National Geospatial-Intelligence Agency

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

Performance Management Standards, Appendix A: Performance Metrics

Overview

The Executive Agents (EAs) have identified, and this Appendix sets forth, a list of minimum performance metrics (or data) that are instrumental to assessing the success of personnel vetting programs and policies. Collection of these metrics will facilitate continuous process improvement by helping to identify potential policy and procedural improvements to enhance program efficiency, effectiveness, fairness, and risk mitigation. The context for each metrics ID describes in detail the information collected to identify these potential improvements.

Departments and Agencies (D/As), investigative service providers (ISPs), authorized adjudicative entities, and shared service providers must collect and provide these performance metrics to the EAs consistent with the reporting schedule outlined in implementation guidance and upon the request of either EA. For each metric, the accountable entity(ies) must be able to distinguish between domains (suitability, fitness, national security, and credentialing) as necessary to provide performance metrics specific to the national security domain to the Security EA and provide performance metrics specific to the suitability, fitness, and credentialing domains to the Suitability and Credentialing EA. The EAs will collect and analyze these performance metrics against the corresponding requirements to monitor and report enterprise implementation of Federal personnel vetting program requirements.

Health Performance Metrics

This category of metrics is used to provide indications of the complexity, productivity, and proficiency of vetting programs and activities.

ID	Metrics	Context	Type	Purpose	Accountable Entity(ies)
HM-01	Number of investigations initiated, pending, discontinued, and completed	Personnel vetting scenario Population type Investigative tier	Efficiency	Help identify investigation inventories and adjudicative program resource needs	D/A ISP

ID	Metrics	Context	Type	Purpose	Accountable Entity(ies)
		Reason for discontinue			
HM-02	Number and percentage of electronic forms submissions rejected	Initiating D/A ISP Reason for rejection	Effectiveness	Helps reflect the quality of investigative forms submissions	D/A ISP
HM-03	Percentage of planned shared service and/or capability uptime	Shared service capability	Efficiency Effectiveness	Helps reflect the availability (uptime) of IT shared services capabilities	Shared service provider
HM-04	Number and percentage of investigations found to have quality concerns	Investigative tier Reason for quality concern	Risk Effectiveness	Helps reflect potential issues with investigative quality and training needs	D/A ISP Authorized adjudicative entity
HM-05	Average time to complete the investigative activity	Investigative Tier Population Type Personnel vetting scenario Supplemental factor, as required	Effectiveness Efficiency	Helps reflect the efficiency of the investigative process both with and without the application of a supplemental factor	ISP
HM-06	Number and percentage of complete and pending adjudications	Personnel vetting scenario Population type	Efficiency Risk	Indicates adjudicative volume, program efficiency, and adjudicative program resource needs	D/A Authorized adjudicative entity

ID	Metrics	Context	Type	Purpose	Accountable Entity(ies)
		Investigative tier Domain Determination (if complete)			Shared service provider
HM-07	Number and percentage of individuals brought on-board with a favorable preliminary determination	Personnel vetting scenario Population type Investigative tier Access level	Risk	Reflects potential risk with individuals for whom an investigation has not been completed having access to people, property, mission, and information	D/A
HM-08	Number and percentage of preliminary determinations with the following outcomes: • Favorable preliminary with favorable final • Favorable preliminary with unfavorable final	Personnel vetting scenario Population type Investigative tier Access level Adjudicative factor	Effectiveness Risk	Indicates realized risk and reflects potential opportunities for continuous process improvement	Authorized adjudicative entity
HM-09	Number and percentage of adverse (e.g. denial, revocation, debarment, removal) or administrative (e.g. suspension, reinstatement) vetting actions	Personnel vetting scenario Population type Investigative tier Action type	Effectiveness Risk	Indicates realized risk and reflects potential opportunities for continuous process improvement of risk management practices	D/A Authorized adjudicative entity

ID	Metrics	Context	Type	Purpose	Accountable Entity(ies)
		Adjudicative factor			
HM-10	Number of exceptions	Personnel vetting scenario	Effectiveness	Supports examination of risk management practices	D/A
		Population type	Risk		Authorized adjudicative entity
		Investigative tier			
		Reason for exception			
HM-11	Number of trust determinations currently undergoing appeal	Personnel vetting scenario	Risk	Provides insight into appeal volumes	D/A
		Population type			Authorized adjudicative entity
		Investigative tier			
		Domain			
		Adjudicative factor			
		Adjudicative entity			
HM-12	Average time to render a personnel vetting determination that supports an on-boarding decision	Personnel vetting scenario	Efficiency	Facilitates analysis of the efficiency and timeliness of on-boarding	D/A
		Population type	Risk		ISP
		Investigative tier[1]			Shared service Provider
		Determination			

---

[1] As defined in the *Federal Personnel Vetting Guidelines*. Investigations conducted prior to the implementation of the *Federal Personnel Vetting Investigative Standards* (legacy investigations) are defined in the *2012 Federal Investigative Standards (FIS)*.

ID	Metrics	Context	Type	Purpose	Accountable Entity(ies)
HM-13	Average time to complete the end-to-end personnel vetting process	Personnel vetting scenario Population type Investigative tier Business function	Efficiency Risk	Indicates the efficiency of personnel vetting programs for each personnel vetting scenario	D/A Shared service provider

Reform Performance Metrics

This category of performance metrics is used to drive implementation, policy decisions, and development of enterprise-wide reforms. Reform performance metrics also measure the implementation and full operating capabilities of emerging reform initiatives or new policy/legislative mandates.

ID	Metrics	Context	Type	Purpose	Accountable Entity(ies)
RM-01	Percentage of investigative data source checks completed using a TIP	Investigative tier Information category	Effectiveness	Provides insight into TIP program effectiveness and impact on operations	Shared service provider ISP
RM-02	Number and percentage of eligible individuals enrolled in Continuous Vetting (CV)	Population type Investigative tier TW state (i.e., TW 1.25, TW 1.5, TW 2.0)	Risk	Reflects compliance with TW 2.0 implementation requirements	D/A ISP

ID	Metrics	Context	Type	Purpose	Accountable Entity(ies)
RM-03	Number and percentage of eligible cases with a successful transfer of trust	Population type Investigative tier	Effectiveness	Facilitates analysis of the effectiveness of the movement of a trusted insider	D/A Authorized adjudicative entity
RM-04	Number and percentage of eligible cases with a successful re-establishment of trust	Population type Investigative tier	Effectiveness	Facilitates analysis of the effectiveness of the process for returning a former trusted insider to work for the Federal Government	D/A Authorized adjudicative entity
RM-05	Number of new CV alerts	Data source Resolution status	Efficiency Effectiveness	Reflects the volume and quality of information provided by CV data sources and indicates resource needs by understanding CV alert volumes and effectiveness of CV data sources	D/A ISP
RM-06	Average time to resolve validated continuous vetting alerts	Population type Investigative tier Information seriousness	Efficiency Risk	Reflects efficiencies and resource needs in CV process	D/A Authorized adjudicative entity ISP
RM-07	Number and percentage of required Annual Vetting Appraisals completed	Investigative tier	Effectiveness	Indicates compliance with TW 2.0 implementation requirements	D/A

ID	Metrics	Context	Type	Purpose	Accountable Entity(ies)
RM-08	Number of D/As using shared services	D/A Shared service capability Business function	Efficiency	Reflects how D/As are leveraging existing resources to reduce costs	Shared service provider
RM-09	Number of requests for supplemental investigative activity	Investigative Tier Data Source	Efficiency Effectiveness	Helps identify trends in requests by D/As to ISPs to supplement investigative results and agency specific information.	ISP

Special Interest Performance Metrics

This category of performance metrics is used to inform policy decisions and program development related to evolving threats, societal trends, research and innovation, or to accomplish process or technology improvements.

ID	Metric	Context	Type	Purpose	Accountable Entity(ies)
SM-01	Population size	Investigative tier Population type Access level	Risk Effectiveness	Informs risk and resource needs	D/A Shared service provider .
SM-02	Costs expended	Vetting scenario Business function Population type	Efficiency	Provides insight into the cost of Federal vetting activities and measures the impact of requirements on resources	D/A ISP Shared Service Providers

ID	Metric	Context	Type	Purpose	Accountable Entity(ies)
		Investigative tier			
SM-03	Number and percentage of issues where an eInterview was used to resolve the issue	Vetting scenario Investigative tier Adjudicative factor	Effectiveness	Reflects the utility of the eInterview capability in the investigative process.	ISP
SM-04	Number of percentage of cases favorably adjudicated by eAdjudication	Investigative tier	Efficiency	Indicates efficiencies of leveraging technology	D/A Authorized adjudicative entity Shared service provider
SM-05	Number of favorable eAdjudication cases re-opened after quality assessment	Investigative tier Reason for re-open	Effectiveness	Helps to ensure quality of automated favorable adjudications	D/A Authorized adjudicative entity Shared service provider ISP

Performance Management Standards, Appendix B: Quality Management Programs

I. Purpose

Entities rely on quality management programs as an internal review mechanism designed to detect and remedy both case-level and systemic problems with personnel vetting programs. Recognizing that, today, most Departments and Agencies (D/A), shared service providers, Investigative Service Providers (ISPs), and authorized adjudicative entities (collectively, covered entities) have some level of quality review for investigations and adjudications, this Appendix identifies the minimum characteristics of quality management programs which will be used by the Security Executive Agent, Suitability and Credentialing Executive Agent, and covered entities to determine the quality of Federal personnel vetting programs.

The parameters introduced in this appendix will help covered entities improve quality, fairness, and consistency in their personnel vetting programs.[1] Covered entities will leverage the key characteristics outlined below to develop their quality management programs.

II. Quality Management Programs

Through well-designed and well-implemented quality management programs, covered entities can proactively identify both problems in individual cases and systemic problems, which may include concerns such as misapplication of investigative standards, adjudicative standards, procedural violations, or barriers in investigative or adjudicatory proceedings. Identifying such problems enable covered entities to ensure adherence to their own policies and improve fairness, perceptions of fairness by individuals, accuracy, inter-decisional consistency, timeliness, and efficiency of their personnel vetting programs, consistent with the Federal Personnel Vetting Core Doctrine.

Each covered entity is required to establish a quality management program which covers the scope of all personnel vetting activities within their organization, including front-end processes, investigations (if applicable), adjudications (if applicable), and personnel vetting management (if applicable).

III. Quality Management Program Key Elements

How covered entities structure their quality management programs can have important consequences for their success. For example, quality management programs that overemphasize timeliness as a measure of quality may overlook problems of decisional accuracy. There are

---

[1] The guidance in this appendix takes into account the recommendations made by the Administrative Conference of the United States (ACUS) 2021-10, *Quality Assurance Systems in Agency Adjudication*, 87 Fed. Reg. 1722 (Jan. 12, 2022). Nevertheless, it was adapted to the special requirements of the personnel vetting enterprise, which differ in important respects from the cases that the ACUS recommendation relied upon.

many methods of quality review that covered entities can use, independently or in combination, depending upon the needs and goals of their programs. This guidance recognizes that covered entities have different quality management needs and available resources. What works best for one covered entity may not work for another. Covered entities must take into account their own unique circumstances when implementing the practices that follow.

A.   Development of Agency Quality Management Programs

1. Covered entities will develop policies and procedures that outline quality management programs that promote fairness, the perception of fairness by the individual, accuracy, inter-decisional consistency, timeliness, efficiency, and other goals relevant to their personnel vetting programs.

2. Covered entities' quality management programs will cover all end-to-end personnel vetting functions within the cognizance of the covered entity.

3. Covered entities' quality management programs will encompass a review of the work of all process areas in the covered entity personnel vetting process and correct deficiencies, as appropriate.

4. Covered entities' quality management programs will include measures to identify training needs and clarify or improve policies.

5. Covered entities' quality management programs will include measures to prepare and circulate regular internal reports that describe systemic trends.

6. Covered entities will determine how information collected through quality management programs will be used to correct problems that impact the fairness or perception of fairness by the individual, accuracy, inter-decisional consistency, timeliness, and efficiency of their programs.

7. Covered entities will design quality management programs to comply with all applicable legal, regulatory, and policy requirements.

8. Covered entities' quality management programs will include measures to validate and verify the quality of contracted support, as appropriate.

9. Covered entities' quality management programs include assessments of whether personnel vetting processes:

a. Accurately determine the facts for the specific matters being reviewed, including validating the identity of the individual;

b. Correctly apply the relevant law, regulation, and policy to the facts of the individual matters;

2

  c. Comply with all applicable personnel vetting requirements;

  d. Are completed in a timely and efficient matter; and

  e. Are consistent and fair across all cases and situations of the same type.

B. Quality Management Personnel

  1. Covered entities will ensure quality management personnel can perform their functions in a manner that is impartial, including being able to perform such functions without pressure, interference, or employment consequences from the personnel whose work they review.

  2. Covered entities will communicate all applicable substantive and procedural requirements to quality management personnel and ensure they have the expertise necessary to review the work of all personnel who have important roles in personnel vetting activities.

  3. Covered entities will ensure quality management personnel have sufficient time to fully and fairly perform their assigned functions.

  4. Quality management personnel will have the expertise and judgment necessary to accurately and impartially perform their responsibilities.

  5. Quality management personnel will use methods for selecting and reviewing cases that allow them to effectively identify case-specific and systemic problems.

  6. Covered entities will ensure quality management personnel have completed appropriate training related to awareness of unconscious bias and ethnic and cultural differences among people to allow them to effectively identify case-specific and systems problems.

C. Timing of and Process for Quality Management Review

  1. Covered entities will consider when quality management reviews should occur for each process area.

  2. Covered entities will consider a layered approach to quality management that employs more than one methodology. As resources allow, this may include formal quality assessments and informal peer review on an individual basis, sampling and targeted case selection on a systemic basis, and case management programs with automated support tools.

  3. In selecting cases for quality management review, covered entities will consider the following methods:

a. Review of every case, which may be useful for covered entities that process a small number of cases but impractical for covered entities that process a high volume of cases;

b. Random sampling, which can be more efficient for covered entities that process a high volume of cases but may cause quality management personnel to spend too much time reviewing cases that are unlikely to present issues of concern;

c. Stratified random sampling, a type of random sampling that over-samples cases based on chosen characteristics, which may help quality management personnel focus on specific issues or known challenges, but may systematically miss certain types of challenges;

d. Targeted selection of cases, which allows covered entities to directly select cases that contain specific case characteristics and may help covered entities study known problems but may miss identifying other possible problems.

D. Performance Metrics Collection and Analysis

1. Covered entities, particularly those with large caseloads, will consider what performance metrics (or data) would be useful and how performance metrics could be used for quality management purposes.

2. Covered entities may develop mechanisms to solicit quality feedback from other data sources (i.e., adjudicative entities) as appropriate to gather required quality performance metrics and should fully utilize existing quality feedback mechanisms such as the Quality Assessment Reporting Tool (QART) or successor capabilities.

3. Covered entities should ensure an electronic case management or other system includes the following information:

a. The identities of any personnel who assisted in gathering, synthesizing, or evaluating information, writing decisions, or performing other case-processing tasks;

b. The procedural history of the case, including any actions and outcomes of administrative or judicial review;

c. The issues presented in the case and how they were resolved;

d. Any other data the agency determines to be helpful.

4. Covered entities will regularly evaluate their electronic case management or other systems to ensure they are collecting the data necessary to assess and improve the quality of decisions in their programs.

5. Covered entities, particularly those with large caseloads, will consider whether to use data analytics and artificial intelligence tools to help quality management personnel identify potential errors or other quality issues. Any use of data analytics or artificial intelligence tools supports, but does not replace, evaluation and judgment by quality management personnel and will be coordinated with the covered entities' privacy and civil liberties professionals, as applicable.

6. Covered entities will ensure that they have the technical capacity, expertise, and data infrastructure necessary to build and deploy necessary performance metrics collection and analysis tools and systems that comply with legal requirements for privacy and security and do not create or sustain harmful biases.

E. Use of Quality Management Data and Findings

1. Covered entities' quality management programs will include capabilities to gather and report data identified in implementation guidance issued by the EAs.

2. Covered entities' quality management programs will include capabilities to gather additional data necessary to manage and operate the covered entities' specific quality management program.

   a. Using the performance metrics gathered, covered entities should propose adjudicative quality metrics to the EAs.

3. Covered entities will not use information gathered through quality management programs in ways that could improperly influence decision making on personnel matters.

4. Covered entities' quality management programs should provide individualized feedback for personnel vetting practitioners within a reasonable amount of time and include any relevant positive and negative feedback.

5. D/As must establish regular communication mechanisms to facilitate the dissemination of various types of quality management information within the agency. Covered entities should:

a. Communicate information about recurring or emerging problems identified by quality management programs to all personnel who participate in the process and to training personnel;

b. Communicate, as appropriate, with the Executive Agents and with policy and operations support personnel to allow them to consider whether recurring problems identified by quality management programs should be addressed or clarified by enterprise policy, covered entity policy, rules, procedures, operational guidance, or decision support tools; and

c. Consider whether to communicate problems identified by quality management programs to agency officials who are positioned to remedy the issue(s).

6. Covered entities must anonymize data from case management programs when making it available for continued research by authorized individuals outside of the agency consistent with appropriate protections unless specifically permitted to share identifiable data.

F.   Assessment and Oversight

1. Covered entities' quality management programs will include periodic assessments of whether systems achieve intended goals, including by affirmatively soliciting feedback from key stakeholders and personnel vetting practitioners concerning the functioning of their quality management programs.

2. Covered entities' quality management programs will support reviews conducted by the EAs related to the quality of their personnel vetting processes and meet all requirements established by the EAs.

3. Covered entities will comply with subsequent implementation guidance issued by the EAs, including any forthcoming guidance that defines the key quality characteristics of each process area (for example, investigations and adjudication) as well as any specific requirements. Covered entities will align their quality management programs with requirements in this appendix and subsequent implementation guidance.

G.   Compliance with Civil Liberties and Privacy Considerations

1. Quality management programs should ensure that the following fundamental civil liberties and privacy principles are applied throughout the personnel vetting enterprise:

a. Privacy documentation: Update or develop a System of Records Notice, as necessary, in accordance with the Privacy Act and implementing regulations.

b. Fairness: Ensure all personnel vetting processes and procedures comply with applicable laws, Executive Orders, and policy regarding the collection, use, retention, and dissemination of protected information.

c. Data quality and accuracy: Ensure that information is accurate by preventing, identifying, and correcting any errors, and making appropriate notification if incorrect information has been shared.