PERSEREC

OPA Report No. 2019-079
PERSEREC-TR-19-06

November 2019

Personnel Security Underreporting: Establishing Rates and Estimating the Problem

Rene M. Dickerhoof
Defense Personnel and Security Research Center
Office of People Analytics

Ray A. Zimmerman
James Beneda
Kimberly M. James
David A. Ciani
Bradley D. Latendresse
Northrop Grumman Technology Services

OPA
OFFICE OF PEOPLE ANALYTICS

Approved for Public Distribution
Defense Personnel and Security Research Center
Office of People Analytics

OPA Report No. 2019-079 **PERSEREC-TR-19-06** **November 2019**

Personnel Security Underreporting: Establishing Rates and Estimating the Problem

Rene M. Dickerhoof
Defense Personnel and Security Research Center, Office of People Analytics

Ray A. Zimmerman, James Beneda, Kimberly M. James,
David A. Ciani, Bradley D. Lattendresse
Northrop Grumman Technology Services

Released by – Eric L. Lang

Defense Personnel and Security Research Center
Office of People Analytics
400 Gigling Road, Seaside, CA 93955

REPORT DOCUMENTATION PAGE	**Form Approved** **OMB No. 0704-0188**

1. REPORT DATE:	2. REPORT TYPE: Technical Report	3. DATES COVERED:
4. TITLE: Personnel Security Underreporting: Establishing Rates and Estimating the Problem	5a. CONTRACT NUMBER: 5b. GRANT NUMBER: 5c. PROGRAM ELEMENT NUMBER:	
6. AUTHOR(S): Rene M. Dickerhoof, Ray A. Zimmerman, James Beneda, Kimberly M. James, David A. Ciani, Bradley D. Lattendresse	5d. PROJECT NUMBER: 5e. TASK NUMBER: 5f. WORK UNIT NUMBER:	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES): Defense Personnel and Security Research Center Office of People Analytics 400 Gigling Road Seaside, CA 93955	8. PERFORMING ORGANIZATION REPORT NUMBER PERSEREC: There are two report numbers: PERSEREC-TR-19-06 OPA Report No. 2019-079	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES):	10. SPONSORING/MONITOR'S ACRONYM(S): 11. SPONSORING/MONITOR'S REPORT NUMBER(S):	
12. DISTRIBUTION/AVAILABILITY STATEMENT: A		
13. SUPPLEMENTARY NOTES:		

ABSTRACT: Prior Defense Personnel and Security Research Center (PERSEREC) research underscores why DoD personnel do not report security-concerning events (see Nelson et al., 2019), but the extent of the problem is unknown. The purpose of this initiative was to determine whether underreporting rates can be computed and to establish these rates, if possible. To this end, PERSEREC isolated all security-reporting requirements elsewhere collected in Defense Manpower Data Center data sources (e.g., sexual assault data are captured in a centralized repository for annual reporting). These and other reportable issues reflect events that should be in DoD's system of record for personnel security tracking and access. Ultimately, PERSEREC focused on five operational data sources and matched these reportable events to corresponding security incidents. These events included sexual assaults (Defense Sexual Assault Incident Database); criminal investigations (Defense Central Index of Investigations); positive drug tests (Military Drug Test File); continuous evaluation alert arrests, warrants, and protection orders (Mirador); and alcoholism, drug, or criminal misconduct Service separations (Active Duty Personnel Transaction File). Results demonstrated that operational data can be matched to security incidents to establish underreporting rates. Indeed, these rates ranged from a low of 65% (65 in 100 not reported) to a high of 99% (99 in 100 not reported) across all examined data sources. Although underreporting is a known issue, these rates were higher than expected given the objective and serious nature of the events examined. Results are discussed in light of data limitations and recommendations are provided for using these underreporting rates to inform process and policy modifications.

14. SUBJECT TERMS:					
15. SECURITY CLASSIFICATION OF: Unclassified			16. LIMITATION OF ABSTRACT:	17. NUMBER OF PAGES: 32	19a. NAME OF RESPONSIBLE PERSON: Eric L. Lang, Director
a. REPORT: Unclassified	b. ABSTRACT: Unclassified	c. THIS PAGE: FOUO			19b. TELEPHONE NUMBER (Include area code): 831-583-2846

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI td. Z39.18

PREFACE

Personnel security underreporting is a well-known problem in the DoD vetting community; however, the Defense Personnel and Security Research Center has never examined whether rates can be established. This study focuses on the underreporting of alleged criminal events (e.g., sexual assaults, drug use, arrest warrants), which represent the *least* subjective and *most* serious security concerns. Establishing reporting rates for these events underscores the extent of the current problem and provides a baseline to measure change in reporting behavior over time. Increasing security reporting is a priority for personnel security professionals, especially as it pertains to criminal issues that have a clear nexus to clearance worthiness.

Eric L. Lang
Director, PERSEREC

EXECUTIVE SUMMARY

Prior Defense Personnel and Security Research Center (PERSEREC) research underscores why DoD personnel do not report security-concerning events (e.g., societal norms not to "snitch," or cultural endorsement of group loyalty over reporting). Yet, no previous research exists to measure how significant this problem is.

This study addressed underreporting by focusing on two research questions. First, can we compute personnel security underreporting rates for known security concerns? Second, if rates can be computed, how significant is the problem? Indeed, results demonstrated that underreporting is the norm rather than the exception, even for serious criminal behavior.

METHOD

To begin this work, PERSEREC considered all personnel-security-reporting requirements explicitly spelled out in policy. PERSEREC then matched these reporting requirements, where possible, to Defense Manpower Data Center (DMDC) operational data sources. For example, sexual assaults must be reported to DoD's personnel security program (PSP) *and* these data are stored in the Defense Sexual Assault Incident Database for annual reporting purposes. Likewise, positive military drug tests must be reported to DoD's PSP *and* these data are captured in a centralized Military Drug Test File. Although these data sources were not designed to inform the PSP directly, they provide objective evidence of events that should be in DoD's system of record for personnel security investigations, adjudications, and incident reporting—the Joint Personnel Adjudication System (JPAS).

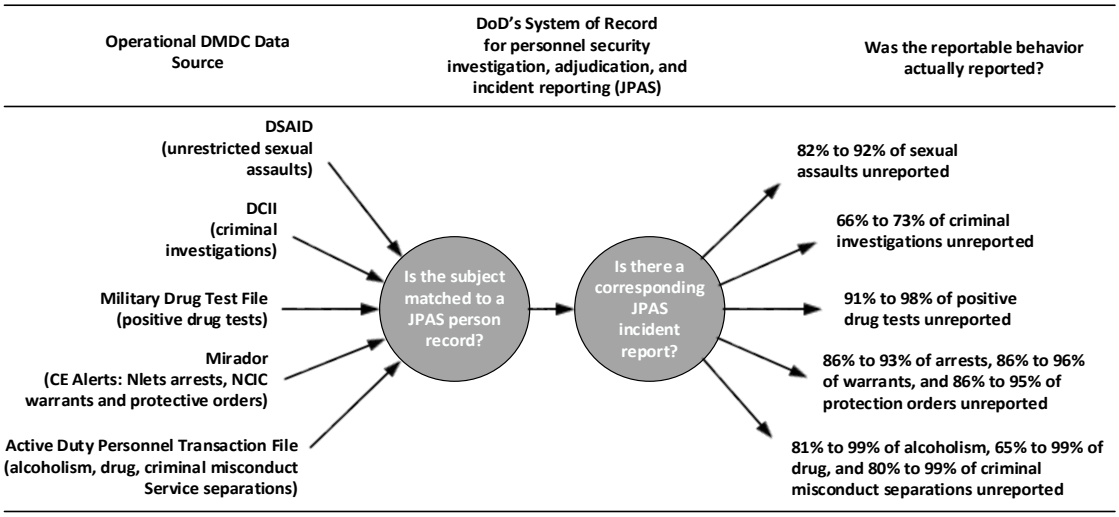
After reviewing relevant Federal Government and DoD-specific security reporting requirements (SEAD 3, DoDM 5200.02), these requirements were matched to reportable events found in DMDC data sources. Specifically, PERSEREC concentrated on five reportable events related to criminal misconduct or substance abuse that should also exist as security incidents. Reportable events included: (a) sexual assaults in the Defense Sexual Assault Incident Database; (b) criminal investigations in the Defense Centralized Index of Investigations; (c) positive drug tests in the Military Drug Test File; (d) continuous evaluation alerts for arrests, warrants, and protection orders in Mirador; and (e) alcoholism, drug, or criminal misconduct separations in the Active Duty Personnel Transaction File.

Although SSN was used to match individuals in DMDC data sources to individuals with a person record in JPAS, additional data processing was needed to determine whether reportable events matched to identified incidents. This matching process was based on the incident's *relevancy to event* and the *reporting interval.* That is, incidents were matched to reportable events if they corresponded to specific Adjudicative Guidelines (e.g., if security managers [SMs] selected Adjudicative Guideline D, E, or J [Sexual Behavior, Personal Conduct, or Criminal Conduct] when entering incident reports for sexual assaults in JPAS). Further, once matched to Adjudicative Guideline(s), incidents had to occur within 1, 2, or 6 months before or after the event.

For example, incident reports related to sexual assault had to occur subsequent to the assault; incident reports related to service separations had to occur prior to the separation.

RESULTS

Matching efforts and analysis of data demonstrated that DMDC data sources can be used to establish underreporting rates for personnel security issues. Indeed, these rates ranged from a low of 65% (65 in 100 not reported) to a high of 99% (99 in 100 not reported) across all examined data sources (see figure below).



DISCUSSION AND RECOMMENDATIONS

Although underreporting is a well-known gap in the personnel security vetting process, rates identified in this study are higher than expected given the objective and severe nature of examined events. Indeed, findings raise serious concerns about adherence to, and effectiveness of, personnel security reporting requirements. Practical actions DoD could undertake to address these rates include:

- Conduct qualitative interviews in the field to understand why criminal and substance abuse behaviors are not reported (identifies process gaps; allows for consideration of whether any reporting requirements should be revised).
- Automate DMDC data sources to feed directly into JPAS or its successor system (bypass human review and discretion for events that are unequivocally reportable).
- Work to professionalize the SM role (e.g., develop a SM desk reference; evaluate whether this position should consistently be a primary job responsibility rather than a collateral duty).
- Build an incident report dashboard to provide up-to-date metrics on security incident reporting; an easy-to-access dashboard would allow DoD to interpret incident report information in real-time to inform policy decision making.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS USED IN THIS REPORT

ACRD	Army Crime Records Directorate
AFOSI	U.S. Air Force Office of Special Investigations
ARC	Automated Records Checks
AWOL	Absent Without Leave
CE	Continuous Evaluation
CY	Calendar Year
DCII	Defense Central Index of Investigations
DMDC	Defense Manpower Data Center
DoDCAF	DoD Consolidated Adjudications Facility
DoDI	DoD Instruction
DoDM	DoD Manual
DSAID	Defense Sexual Assault Incident Database
FY	Fiscal Year
ISC	Inter-service Separation Code
IT	Information Technology
JPAS	Joint Personnel Adjudications System
LIMS	Laboratory Information Management System
MPDATP	Military Personnel Drug Abuse Testing Program
NCIC	National Crime Information Center
NCIS	Naval Criminal Investigative Service
NDAA	National Defense Authorization Act
NGA	National Geospatial-Intelligence Agency
Nlets	The International Justice and Public Safety Network
NRO	National Reconnaissance Office
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OPA	Office of People Analytics
OUSD(I)	Office of the Undersecretary of Defense for Intelligence
PAC	Performance Accountability Council
PERSEREC	Defense Personnel and Security Research Center
PSP	Personnel Security Program
SAPR	Sexual Assault Prevention and Response
SAPRO	Sexual Assault Prevention and Response Office
SCI	Sensitive Compartmented Information
SEAD	Security Executive Agent Directive
SF-86	Standard Form 86
SM	Security Manager
SSN	Social Security Number

INTRODUCTION

Over the years, PERSEREC has conducted several studies to address why DoD employees do not report security-concerning information in the workplace. This research points to a variety of factors including personal dynamics (e.g., relationship to the wrongdoer), situational cues (e.g., ambiguity over seriousness or relevance of issue), organizational climate (e.g., cultural endorsement of group loyalty over reporting), and societal norms (e.g., long-engrained conditioning not to "snitch" or "tattle").[1] Although we now have a reasonable grasp on what perpetuates this problem, the extent of underreporting and the degree of threat it presents to national security remain unknown.

The purpose of the current study is to estimate security underreporting by comparing reportable events identified in DMDC-owned or -operated data sources (e.g., law enforcement, program management, or human resource data) to those formally entered into DoD's system of record for personnel security investigations, adjudications, and incident reporting (JPAS). Although operational DMDC data sources are not intended to capture reportable events for personnel security purposes, they can inform security incident reporting rates. That is, a reportable issue recorded in another data source that is not associated with a JPAS personnel security incident indicates a failure to report. Comparing reportable issues found in DMDC data sources to those recorded in JPAS provides DoD with a baseline assessment of underreporting and a clearer understanding of the risk associated with this issue.

JPAS consists of an application for entering and tracking information and a database for storing such information. In addition to current and historical clearance and access information, JPAS maintains records concerning security incidents and subsequent adjudications. When security officials become aware of reportable issues—either self-, coworker-, commander-, or supervisor-reported—DoD policies require security officials to establish a JPAS incident for adjudicative review by DoDCAF. The extent to which SMs, commanders, and supervisors are not made aware of these security concerns, or choose not to submit them, needs to be known.

POLICY BACKGROUND

In 2013, the President of the United States directed OMB to review suitability and security procedures across the Federal Government. The purpose of this effort was to inform new priorities for process reform. The subsequent review (OMB, 2014) indicated need to "clarify and expand requirements for reporting actions and events of employees and contractors to support decisions on access to facilities, classified/sensitive information, and IT systems." Recommendations included implementation of uniform

[1] For an overview of previous PERSEREC research on reporting events, as well as an in depth review of academic literature on the topic, see Nelson, Beneda, McGrath and Youpa (2019).

Federal-Government-wide reporting requirements tiered by person risk or eligibility level.

In response to this recommendation, SEAD 3, *Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position*, was published by ODNI in 2017 (ODNI, 2017a). In conjunction with these Federal reporting requirements, and to implement this Federal directive at the agency level, DoD added CE reporting requirements to its PSP manual, DoDM 5200.02, *Procedures for the DoD Personnel Security Program (PSP)* (DoD, 2017c). Both of these sources identify specific events, behaviors, or observations that covered individuals are expected to report. In addition to these new resources, DoD also issued specific reporting requirements for individuals with access to SCI in DoDM 5105.21, Vol. 3 (DoD, 2018c).

Although reporting requirements are now explicitly listed in Federal and DoD policies, many of these reportable issues are not, by their nature, recorded in any operational systems. For example, it would be difficult to identify "failure to report blackmail" unless it is uncovered during a periodic reinvestigation via a secondary source (e.g., a friend or confidante). Likewise, no operational system exists to capture concerning personality disorders, misuse of IT systems, or existence of foreign national roommates.

However, some reporting requirements do lend themselves to large-scale assessment for the purposes of measuring underreporting. For example, SEAD 3 (ODNI, 2017a) states that criminal conduct must be reported for all covered individuals *and* Mirador collects records of criminal offenses identified in multiple criminal history data sources (e.g., NCIC, Nlets). Mirador data can be used to identify whether a corresponding JPAS personnel security incident was ever established.

CURRENT STUDY

This study was funded by OPA in support of efforts to continuously improve DoD's PSP. Although funded by OPA, SAPRO acted as a functional sponsor for this work to better understand whether alleged sexual assaults are being routed to the personnel security program for awareness and adjudication. This report addresses two specific research questions:

1. Can personnel security underreporting rates be computed?
2. If identifiable, what are these reporting rates?

Estimating underreporting rates provides a baseline assessment of this problem now that specific reporting requirements are in place at Federal and DoD levels. These rates can help identify reporting gaps and inform policy change or future trend analyses. One of the primary reform goals put forth by the PAC is to increase availability and quality of critical personnel security information to improve decision making. On behalf of OPA and PERSEREC, the purpose of this research initiative is to do just that.

METHOD

This section breaks down the study methodology into four components:

- The policy review that provided the foundation for the study;
- The identified data sources, their respective data elements, and the data preparation and matching procedures;
- The sample timeframes for each of the five identified data sources and a breakdown of subject affiliations across a combined sample (e.g., Service member, civilian, contractor); [2] and
- An outline of the analytic strategy used to estimate reporting rates.

POLICY REVIEW

The initial step for this research was to review policies related to personnel security reporting requirements. The purpose of the review was to (a) identify all explicit reporting requirements codified in policy and (b) link those requirements to reportable events identified in other accessible DMDC data sources. Ultimately, SEAD 3 (ODNI, 2017a), DoD's PSP Manual, and DoDM 5105.21 (DoD, 2018c) fully covered all reportable personnel security concerns. For each of these policies, all plain-language-reporting requirements were extracted and a table was created listing each requirement under its corresponding policy source. The requirements extracted from these sources are listed in Table 1.

[2] Analyses were performed separately for each data source sample. Samples were combined only to show a breakdown of affiliations for all subject data used in the study.

Table 1
Federal and DoD Reporting Requirements

SEAD 3 Federal Requirements for All Covered Individuals	SEAD 3 Federal Requirements for Individuals With Access to Secret or Confidential Information	DoDM 5200.02 Requirements for All Covered Individuals	DoDM 5105.21-V3 Requirements for Individuals Requiring SCI Access (not to include NSA, NGA, or NRO)
Reportable actions for self: • Official Duty Foreign Travel (reporting requirement determined by agency) • Unofficial Foreign Travel (submit itinerary to agency head, approval then required) • Official Duty Foreign Contacts (reporting requirement determined by agency) • Unofficial Foreign Contacts (foreign intelligence entities and foreign nationals involving intimate or personal contact) Reportable actions by others: • Unwillingness to comply with rules and regulations or to cooperate with security requirements • Unexplained affluence • Alcohol abuse • Illegal use or misuse of drugs or drug activity • Appearance of suspected mental health issues where there is reason to believe it may impact the covered individual's ability to protect classified information • Criminal conduct • Any activity that raises doubts as to whether another covered individual's continued national security eligibility is clearly consistent with the interests of national security • Misuse of U.S. Government property or information systems	All SEAD 3 covered individual reporting requirements plus: • Application for and receipt of foreign citizenship • Application for, possession of, or use of a foreign passport or identity card for travel • Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified information • Media contacts (other than for official purposes), where the media seeks access to classified information • Arrests • Bankruptcy or over 120 days delinquent on any debt • Alcohol-and drug-related treatment **SEAD 3 Requirements for Individuals With Access to Top Secret Information** All SEAD 3 covered individual and secret/ confidential reporting requirements plus: • Direct involvement in foreign business • Having a foreign bank account • Ownership of foreign property • Voting in a foreign election • Adoption of non-U.S. citizen children • Financial anomalies such as garnishments or any unusual infusion of assets $10K or greater such as an inheritance, winnings, or similar financial gain • Foreign national roommate(s) • Cohabitant(s) • Marriage (marital changes)	All SEAD 3 reporting requirements plus: • Any incident or behavior identified in the August 30, 2006 OUSD(I) Memorandum; Intelligence Community Policy Guidance 704.1 (ODNI, 2008); and DoD 5220.22-R (DoD, 2018b) • Investigation of Government travel card misuse, abuse, or fraud • Information that suggests an individual may have an emotional, mental, or personality condition that can impair judgment, reliability, or trustworthiness. • A known history of mental disorder • A reporting that an individual has sought treatment for a mental, emotional, or substance abuse condition (commensurate with any reporting limitations of Section 21 on the SF-86) • Direct and indirect threats of violence • Physical altercations, assault, or significant destruction of U.S. Government property • An abrupt and significant change in an individual's appearance or behavior suggesting impaired judgment or stability • Signs of substance use or intoxication on the job • An indication of substance abuse after completion of treatment • Evidence of alcohol or drug related behavior outside the workplace • Suicide threats, attempts, gestures, or actions • Any other behaviors that appear to be abnormal and indicate impaired judgment, reliability, or maturity	All SEAD 3 reporting requirements plus: • Outside employment related to discussion, publication, or analysis of material on intelligence, defense, or foreign affairs • Bankruptcy filing • Credit judgments • Excessive debt • Foreclosure • Repossessions • Tax liens • Wage garnishments • Anticipated foreign travel • Outside employment with foreign interest • Outside employment with the government of a foreign nation • Change in association with foreign nationals • Illegal or unauthorized access sought • Invitations from foreign government officials or foreign intelligence entity • Legal name change • Change in marital status • Intent to marry or cohabitate with a foreign individual • Adverse involvement with law enforcement (excluding traffic incidents under $300) • Additional foreign travel experiences to include whether one was a victim of or witness to any criminal activity

DATA SOURCES

To identify the data sources for this study, DMDC's catalogue of application databases and mainframe files was examined and the written summary for each data source was reviewed. From these descriptions, it was determined that the majority of data sources did not contain information relevant to personnel security reporting requirements. For

those that did contain relevant information, record layouts and other available information on DMDC's website were examined to find relevant data elements. Ultimately, five data sources containing reportable events were selected. All sources applied to alleged criminal misconduct or substance abuse.

Finally, underreporting was examined by matching events identified in these five DMDC data sources to a criterion—experience of a JPAS incident report. The JPAS operational database, the procedures for matching reportable events to JPAS incidents, and the five identified DMDC data sources are described next.

Joint Personnel Adjudication System

JPAS is a DMDC application for entering, updating, and maintaining information related to security clearance investigations and eligibility determinations for DoD military, civilian, and contractor personnel. It includes the capability for SMs to update individual records, including entry of personnel security incidents. JPAS was developed for operational use by SMs and other end users. PERSEREC receives an extract of DMDC JPAS records roughly every 6 months for research purposes.

For this study, JPAS records served as the base population of DoD personnel who are subject to the reporting requirements listed in Table 1.[3] Personnel security incident reports are created by SMs in an individual's JPAS record. The incident report includes the incident date and the SEAD 4 Adjudicative Guidelines (ODNI, 2017b) deemed relevant by the SM.

In this study, JPAS incident reports used were the criterion measure for compliance with personnel security reporting requirements. For instance, a Service member who tests positive for illegal drug use under MPDATP (DoD, 2018a) should have a corresponding JPAS incident report. The JPAS sample for this study included all JPAS records provided in the DMDC November 2018 extract.

Overview of Matching Procedures

No standard procedures currently exist for linking reportable events in DMDC data sources to incident reports in JPAS. SSN was used to match individuals in DMDC data sources to individuals with a person record in JPAS, but additional data processing was needed to determine whether the reportable events were likely matches to each incident. A matching strategy was developed based on two assumptions.

The first assumption was that matches based on relevant SM-selected adjudicative guidelines in JPAS are more likely to be true matches than guidelines having no relationship to the event. For example, when matching a sexual assault to a JPAS incident report, a match based on Guideline J: Criminal Conduct is likely a true match, while one based on Guideline M: Use of Information Technology is likely a false

[3] This population does not include the DoD Intelligence Community.

match. Guideline D: Sexual Behavior may also provide a true match in the case of a sexual assault, either by itself or in combination with Guideline J. Guideline E: Personal Conduct was also included in matching procedures after reviewing the frequency distribution of all incident reports by adjudicative guidelines and noting widespread use of this guideline by SMs. The SM-selected adjudicative guidelines used for matching data source events to incident reports are listed in Table 2.

Table 2
DMDC Data Sources, Reportable Events, and Incident Adjudicative Guidelines

Data Source	Reportable Event	Relevant Adjudicative Guideline
DSAID	Sexual Assault	D: Sexual Behaviors
		E: Personal Conduct
		J: Criminal Conduct
DCII	Criminal Investigation	E: Personal Conduct
		J: Criminal Conduct
Military Drug Test File	Positive Drug Test	E: Personal Conduct
		H: Drug Involvement and Substance Misuse
		J: Criminal Conduct
Mirador	CE Alert: Arrest Record (Nlets)	E: Personal Conduct
		J: Criminal Conduct
	CE Alert: Warrant Issued (NCIC)	E: Personal Conduct
		J: Criminal Conduct
	CE Alert: Protection Order Issued (NCIC)	E: Personal Conduct
		J: Criminal Conduct
Active Duty Personnel Transaction File	Separation: Alcoholism	E: Personal Conduct
		G: Alcoholism
	Separation: Drugs	E: Personal Conduct
		H: Drug Involvement and Substance Misuse
	Separation: Criminal Misconduct	E: Personal Conduct
		J: Criminal Conduct

The second assumption made was that matches based on shorter time periods between a reportable event and a JPAS incident report are more likely to be true matches relative to those that are temporally distant. For DSAID, the Military Drug Test File, and Mirador data sources, incident reports (with the appropriate adjudicative guidelines) created at 1, 2, and 6 months *following* the data source event date were classified as true matches. For Service separations (from the Active Duty Transaction File), incident reports (with the appropriate adjudicative guidelines) identified at 1, 2, and 6 months *preceding* the data source event date were classified as true matches. DCII records were matched to JPAS incidents occurring in the same or following year because these investigations are catalogued by year alone. Ultimately, the methodology applied in this study, as depicted in Figure 1, was a targeted approach to minimize false and maximize true matches.

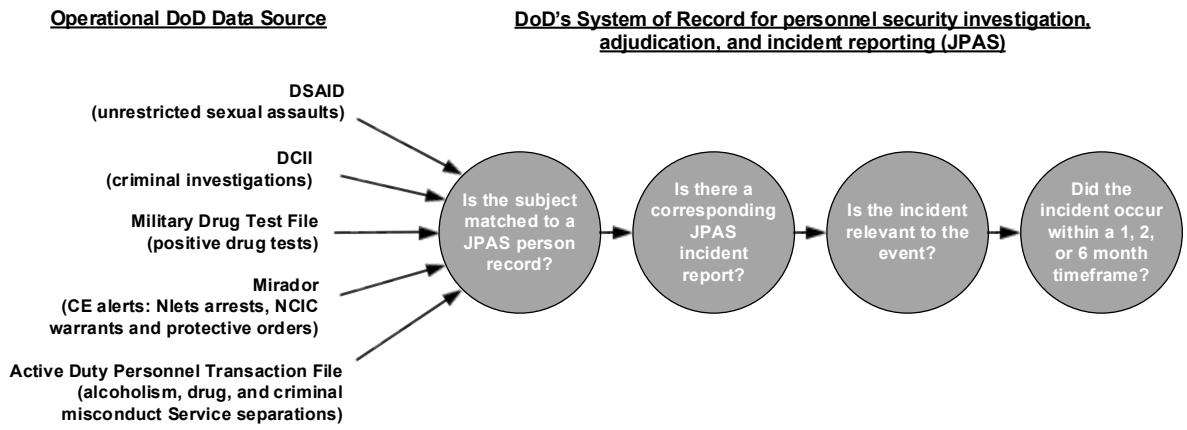


Figure 1 Methodological Model to Establish Reporting Rates Using JPAS Incidents as Criterion Measure

Defense Sexual Assault Incident Database

DSAID is the DoD system of record for information collected through its SAPR program (DoDI 6495.02, [DoD, 2017b]). DSAID was developed to meet FY09 NDAA requirements to provide a centralized database for information related to sexual assaults (Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 [2008]). DSAID reports can be Unrestricted or Restricted. Unrestricted reports trigger an investigation and command notification, whereas Restricted reports remain confidential within the SAPR program. DSAID alleged sexual assaults are generally reported to a Component SAPR program by the victim; however, DSAID also receives records of Unrestricted reports made directly to military law enforcement agencies. Ultimately, the victim always decides whether their report will be Unrestricted or Restricted.

Records for all Unrestricted reports in DSAID, from CY14 through CY17, were accessible for this study. The DSAID Control Number—the unique identifier for an assault—was used to link assaults to alleged perpetrators. Assaults involving multiple perpetrators were treated as multiple assaults. For instance, if two alleged perpetrators were involved in an assault, two separate assault records were created—one for each perpetrator. The assault records were then matched by the perpetrator's SSN to JPAS.

Matches between DSAID assault records and corresponding JPAS incidents were based on SM-selected adjudicative guideline (separately and in combination) as presented in Table 2. Estimated reporting rates were then calculated for matched incidents occurring 1, 2, and 6 months after the DSAID event date.

Defense Central Index of Investigations

DCII is a database containing case file numbers and other summary information from investigations conducted by a number of DoD agencies. These include personnel security background, counterintelligence, and criminal investigations. It functions solely as an index to the investigative case files that are maintained by the respective investigative agencies (e.g., AFOSI, NCIS, and ACRD). Per DoDI 5505.07 (DoD, 2018d),

criminal investigations conducted by DoD agencies must be indexed "as soon as the investigation determines there is credible information that the subject committed a criminal offense." Indexes of personnel security background investigations and counterintelligence investigations do not specifically indicate reportable events and were beyond the scope of this study.

A DCII extract of investigations indexed from CY14 through CY17 by ACRD,[4] NCIS, and AFOSI was obtained for this study. NCIS and AFOSI conduct all three types of investigation, while ACRD indexes are restricted to criminal investigations. Because DCII does not clearly distinguish the type of investigation for a given case index, NCIS and AFOSI investigations data could not be included in this study. Thus, the DCII sample for this study included all ACRD records indexed in DCII from CY14 through CY17. These records were matched by SSN to the JPAS dataset to identify criminal investigation records for covered individuals.

Matches between DCII criminal investigation records and corresponding JPAS incidents were based on SM-selected adjudicative guidelines (separately and in combination) as presented in Table 2. Estimated reporting rates were then calculated for incidents dated within the same or following year of the DCII investigation because DCII does not provide exact event dates.

Military Drug Test File

The Military Drug Test File contains drug test results conducted on Active Duty Service members. LIMS controls and maintains this database for the MPDATP (DoDI 1010.01 [DoD, 2018a], DoDI 1010.16 [DoD, 2017a]). LIMS sends positive drug test results to commands within 6 days; negative or inconclusive results are sent within 4 days. All test results for a given quarter are provided to DMDC, which maintains the Military Drug Test File. To expedite the receipt of data from this file, data were requested from OPA's Data Science Division rather than from DMDC. Although the records in this file date back to the 1990s, OPA's extract, at the time of the request, contained records only from January 1, 2016 through June 30, 2018.

From this dataset, all records for which the test result date (i.e., the date the result was reported to the subject's command) occurred in CY16 or CY17 were selected. Records for non-positive test results (i.e., the result code was Negative, Discrepant, or Invalid Value) were discarded and remaining Positive records were matched by SSN to the JPAS dataset.

Matches between positive test result records and corresponding JPAS incidents were based on SM-selected adjudicative guidelines (separately and in combination) as

[4] ACRD was reorganized as the Army Crime Records Center. DCII documentation, however, continues to describe the data source as ACRD.

presented in Table 2. Estimated reporting rates were then calculated for matched incidents occurring 1, 2, and 6 months after the test result date.

Mirador

Mirador is DMDC's system for compiling and validating ARCs for DoD's CE program. CE alerts are generated for reports meeting minimum thresholds. Alerts are reviewed by an independent validation cell, which conducts identity resolution, determines if the report exists in other data sources, and assigns an adjudicative guideline for cases meeting minimum thresholds (Morse et al., 2019).

Nlets provides Mirador with arrest records and other criminal history data from local, State, and Federal law enforcement agencies. NCIC provides records for arrest warrants and protection orders. The Mirador sample for this study included records from Nlets and NCIC for events that occurred from FY15 through FY17.

Matches between Mirador CE alert records and corresponding JPAS incidents were based on SM-selected adjudicative guidelines (separately and in combination) as presented in Table 2. Estimated reporting rates were then calculated for matched incidents occurring 1, 2, and 6 months after the Mirador event date.

Active Duty Personnel Transaction File

The Active Duty Personnel Transaction File contains personnel data provided to DMDC by each of the Services. It contains records of separation from active duty. These records include the reason for separation (i.e., separation code) and the date the separation occurred. Because each Service has its own separation codes, DMDC created and maintains a DoD-wide set of ISCs that map to Service-specific codes.

The sample for this study included all active duty separations for alcoholism, drugs, or broad criminal misconduct occurring from FY15 through FY17. The specific reasons for separation and ISCs examined for this study are listed in Table 3.

Table 3
Interservice Separation Codes Employed in This Study

Reason for Separation	ISC	ISC Descriptor
Alcoholism	1064/2064	Alcoholism
Drugs	1067/2067	Drugs
Criminal Misconduct	1071/2071	Civil Court Conviction
Criminal Misconduct	1073/2073	Court Martial
Criminal Misconduct	1075/2075	AWOL, Desertion
Criminal Misconduct	1078/2078	Good of the Service (In lieu of Court-Martial)
Criminal Misconduct	1084/2084	Commission of a Serious Offense
Criminal Misconduct	1101/2101	Dropped from Strength for Desertion
Criminal Misconduct	1102/2102	Dropped from Strength for Imprisonment

These separations were matched to JPAS using SSN. Matches for each separation cause (i.e., alcoholism, drugs, criminal misconduct) and corresponding JPAS incidents were based on SM-selected guidelines (separately and in combination) as presented in Table 2. Estimated reporting rates were then calculated for matched incidents occurring 1, 2, and 6 months before the separation date.

SAMPLE

Timeframes for JPAS and DMDC data source samples are displayed in Figure 3. JPAS incident data covered all DMDC data source timeframes plus and minus at least 6 months. That is, incident data were available at least 6 months *after* events identified in DSAID, DCII, the Military Drug Test File, and Mirador and at least 6 months *before* any relevant separation found in the Active Duty Personnel Transaction File.

Data Source	Time Period	Begin Date	End Date
JPAS		4/1/2013	11/1/2018
DSAID	CY14-CY17	1/1/2014	12/29/2017
DCII	CY14-CY17	1/1/2014	12/29/2017
Military Drug Test File	CY16-CY17	1/1/2016	12/29/2017
Mirador	FY15-FY17	10/1/2014	9/29/2017
Active Duty Personnel Transaction File	FY15-FY17	10/1/2014	9/29/2017

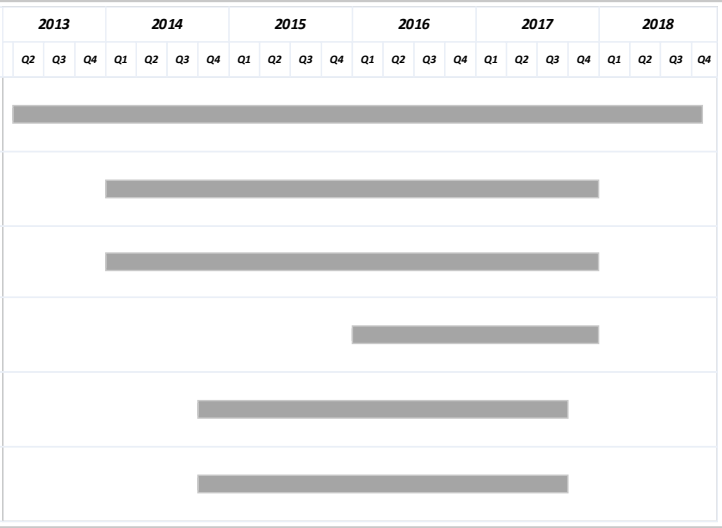


Figure 2 Timeframes for Data Sources by Calendar Year

JPAS data were used to calculate the frequency distribution of subject affiliations with reportable events as shown in Table 4. In this table, all five DMDC data source samples are combined to provide subject affiliations on the whole rather than within each data source. Importantly, however, all study analyses were performed separately for each data source sample.

Note that affiliations are not mutually exclusive. For instance, an individual could be a full-time Government civilian while serving in the National Guard. Therefore, individuals with more than one affiliation are counted more than once and the frequencies presented in Table 4 are greater than the actual number of individual subjects examined (Total n = 200,215).

As indicated in Table, the combined sample is heavily weighted toward military personnel. Even when considering the possibility of multiple affiliations, Government civilians and contractors are underrepresented. This is not surprising, however,

because the Military Drug Test File and the Active Duty Personnel Transaction File contain information only on Service personnel.

Table 4
Subjects With Reportable Events by Affiliation

Affiliation	**n**[3]
Military	189,553
Government Civilian	10,452
Contractor	7,381
Coast Guard[1]	306
Uniformed Public Health Service[1]	1
Unknown[2]	1,123

[1] The population also included a small number of DoD-affiliated personnel to include some Coast Guard subjects and one Uniformed Public Health Service employee.

[2] 1,123 subjects did not possess an affiliation (Unknown in JPAS).

[3] 8,591 subjects were affiliated as both a Service member and a civilian; 10 subjects were both in the Coast Guard and a civilian.

RESULTS

This section describes JPAS incident reporting rates based on reportable events captured in DMDC data sources and matched to JPAS incidents. Each subsection provides the following information:

- Number of reportable events in the DMDC data source,
- Number of reportable events matched to incident reports in JPAS,
- Range of reporting rates for SM-selected adjudicative guidelines and reporting intervals, and
- Summary of underreporting rates for the reportable event.

DEFENSE SEXUAL ASSAULT INCIDENT DATABASE

We identified 21,362 unrestricted sexual assault records in DSAID. Of these subjects, 9,523 subjects with an assault date record and perpetrator SSN matched to a JPAS person record.[5] Table 5 provides the reporting rates by SM-selected adjudicative guideline and reporting interval. The reporting range across all SM-selected guidelines and reporting intervals was 7.8% to 18.8%. This range suggests that as many as 92% (or as few as 82%) of assault events go unreported in JPAS.

Table 5
CY14-CY17 Personnel Security Reporting Rates for Alleged Sexual Assaults

(n = 9,523)	Reporting Interval					
SM-Selected Adjudicative Guideline	Within 1 Month		Within 2 Months		Within 6 Months	
	n	%	n	%	n	%
D: Sexual Behaviors	948	10.0	1,059	11.1	1,324	13.9
E: Personal Conduct	802	8.4	939	9.9	1,245	13.1
J: Criminal Conduct	742	7.8	852	8.9	1,074	11.3
Any or All of the Above	1,195	12.5	1,375	14.4	1,786	18.8

DEFENSE CENTRAL INDEX OF INVESTIGATIONS

For ACRD, NCIC, and AFOSI combined, we identified 225,360 subject investigations in DCII. Of these subjects, 150,528 were associated with a JPAS person record. Of those with JPAS records, only 78,484 applied to ACRD investigations. Table 6 displays the reporting rates for these 78,484 ACRD investigations by SM-selected adjudicative guideline and reporting interval. Reporting rates ranged from 26.7% to 33.8%. This

[5] The complete dataset provided by SAPRO contained 6,435 records that did not possess an assault incident date. From there, 5,190 additional records could not be matched to JPAS due to missing SSNs for alleged perpetrators. Finally, 214 records pertained to alleged perpetrators who did not have a JPAS record.

range suggests that as many as 73% (or as few as 66%) of ACRD investigations go unreported in JPAS.

Note that DCII records are indexed by year only. Given this, we counted JPAS incidents dated in the same or following year as potential matches. This extended reporting interval (potentially up to 2 years), relative to other data sources, increased the likelihood of matching JPAS incident reports to DCII investigations. As a result, the reporting rates in Table 6 may be inflated.

Table 6
CY14-CY17 Personnel Security Reporting Rates for Criminal Investigations

(n = 78,484)	Reported Within 2 Years	
SM-Selected Adjudicative Guideline	**n**	**%**
E: Personal Conduct	23,033	29.3
J: Criminal Conduct	20,926	26.7
Any or All of the Above	26,515	33.8

MILITARY DRUG TEST FILE

We identified 65,044 positive drug test results; 64,918 applied to subjects with a JPAS person record. Table 7 provides the reporting results by SM-selected adjudicative guideline and reporting interval. The reporting range across SM-selected guidelines and reporting intervals was 1.6% to 9.3%. This range suggests that as many as 98% (or as few as 91%) of positive drug test results go unreported in JPAS.

Table 7
CY16-CY17 Personnel Security Reporting Rates for Positive Drug Tests

(n = 64,918)	Reporting Interval					
	Within 1 Month		Within 2 Months		Within 6 Months	
SM-Selected Adjudicative Guideline	**n**	**%**	**N**	**%**	**n**	**%**
E: Personal Conduct	1,591	2.5	2,104	3.2	2,885	4.4
H: Drug Involvement and Substance Misuse	3,503	5.4	4,287	6.6	5,440	8.4
J: Criminal Conduct	1,022	1.6	1,442	2.2	1,981	3.1
Any or All of the Above	3,746	5.8	4,649	7.2	6,065	9.3

MIRADOR

Table 8 displays the JPAS incident reporting rates for Mirador CE alerts involving Nlets arrests, NCIC warrants, and NCIC protection orders. The rates are provided by SM-selected Adjudicative Guidelines and reporting interval.

We identified 775 total Nlets arrest records; 687 applied to subjects with a JPAS person record. The reporting range across SM-selected adjudicative guidelines and reporting

intervals was 7.1% to 14.3%. This suggests that as many as 93% (or as few as 86%) of arrests identified by Nlets go unreported in JPAS.

We identified 122 NCIC arrest warrant records; 118 applied to subjects with a JPAS person record. The range over all SM-selected adjudicative guidelines and reporting intervals was 4.2% to 14.3%. This suggests that as many as 96% (or as few as 86%) of warrants identified by NCIC go unreported in JPAS.

We identified 203 NCIC protection order records; 182 applied to subjects with a JPAS person record. The range across SM-selected adjudicative guidelines and reporting intervals was 4.9% to 14.3%. This suggest that as many as 95% (or as few as 86%) of protection orders identified by NCIC go unreported in JPAS.

Table 8
CY14-CY17 Personnel Security Reporting Rates for Arrests, Warrants, and Protection Orders

Nlets Arrests (n = 687)	**Reporting Interval**					
	Within 1 Month		**Within 2 Months**		**Within 6 Months**	
Adjudicative Guideline	**n**	**%**	**n**	**%**	**n**	**%**
E: Personal Conduct	49	7.1	53	7.7	59	8.6
J: Criminal Conduct	76	11.1	80	11.6	84	12.2
Any or All of the Above	88	12.8	92	13.4	98	14.3
NCIC Warrants (n = 118)	**Reporting Interval**					
	Within 1 Month		**Within 2 Months**		**Within 6 Months**	
Adjudicative Guideline	**n**	**%**	**n**	**%**	**n**	**%**
E: Personal Conduct	5	4.2	5	4.2	6	5.1
J: Criminal Conduct	6	5.1	6	5.1	7	5.9
Any or All of the Above	6	5.1	6	5.1	7	14.3
NCIC Protection Orders (n = 182)	**Reporting Interval**					
	Within 1 Month		**Within 2 Months**		**Within 6 Months**	
Adjudicative Guideline	**n**	**%**	**n**	**%**	**n**	**%**
E: Personal Conduct	9	4.9	9	4.9	11	6.0
J: Criminal Conduct	13	7.1	13	7.1	17	9.3
Any or All of the Above	15	8.2	15	8.2	19	14.3

ACTIVE DUTY PERSONNEL TRANSACTION FILE

Table 9 displays the JPAS incident reporting rates for Service separations related to alcoholism, drugs, or criminal misconduct.[6] These rates are categorized by SM-selected Adjudicative Guideline and reporting interval.

We identified 2,958 Service separations related to alcoholism; 2,957 applied to subjects with a JPAS person record. The reporting range across SM-selected adjudicative guidelines and reporting intervals was 1.2% to 19.1%. This range suggests that as many as 99% (or as few as 81%) of events resulting in an alcoholism-related separation go unreported in JPAS.

We identified 20,879 Service separations related to drugs; 20,875 applied to subjects with a JPAS person record. The reporting range across SM-selected adjudicative guidelines and reporting intervals was 1.4% to 35.0%. This range suggests that as many as 99% (or as few as 65%) of events resulting in a drug-related separation go unreported in JPAS.

We identified 27,389 Service separations for criminal misconduct; 27,368 applied to subjects with a JPAS person record. The reporting range across SM-selected adjudicative guidelines and reporting intervals was 1.2% to 19.7%. This range suggests that as many as 99% (or as few as 80%) of events resulting in a separation due to criminal misconduct go unreported in JPAS.

[6] Table 3 of the Method section provides the ISCs used to identify separations for alcoholism, drugs, and criminal misconduct.

Table 9
FY15-FY17 Personnel Security Reporting Rates for Alcohol, Drug, and Misconduct-related Separations

Alcohol-Related (n = 2,957)	Time From JPAS Report Until Separation					
Adjudicative Guideline	**Within 1 Month**		**Within 2 Months**		**Within 6 Months**	
	n	**%**	**n**	**%**	**n**	**%**
E: Personal Conduct	35	1.2	103	3.5	425	14.4
G: Alcohol Consumption	48	1.6	115	3.9	437	14.8
Any or All of the Above	56	1.9	145	4.9	564	19.1
Drug-Related (n = 20,875)	**Time From JPAS Report Until Separation**					
Adjudicative Guideline	**Within 1 Month**		**Within 2 Months**		**Within 6 Months**	
	n	**%**	**n**	**%**	**n**	**%**
E: Personal Conduct	284	1.4	844	4.0	4,616	22.1
H: Drug Involvement & Substance Use	459	2.2	1,383	6.6	6,844	32.8
Any or All of the Above	482	2.3	1,454	7.0	7,308	35.0
Criminal Misconduct (n = 27,368)	**Time From JPAS Report Until Separation**					
Adjudicative Guideline	**Within 1 Month**		**Within 2 Months**		**Within 6 Months**	
	n	**%**	**n**	**%**	**n**	**%**
E: Personal Conduct	488	1.8	1,118	4.1	4,836	17.7
J: Criminal Conduct	320	1.2	713	2.6	3,528	12.9
Any or All of the Above	538	2.0	1,234	4.5	5,388	19.7

SUMMARY OF UNDERREPORTING

Table 10 summarizes the underreporting findings across all five data sources. Overall, levels of underreporting were much higher than expected. According to personnel security policy requirements reviewed in this study (SEAD 3; DoDM 5200.02; DoDM 5105.21-V3), no such information should go unreported.

Table 10
Underreporting Rates by DMDC Data Source

Data Source	Information Type	% Unreported (Range)
DSAID	Unrestricted Sexual Assault Report	82 to 92
DCII	Evidence of Criminal Misconduct	66 to 73
Military Drug Test File	Positive Drug Test Result	91 to 98
Nlets	Arrest	86 to 93
NCIC	Warrant	86 to 96
NCIC	Protection Order	86 to 95
Active Duty Personnel Transaction File	Service Separation Due to Alcoholism	81 to 99
Active Duty Personnel Transaction File	Service Separation Due to Drugs	65 to 99
Active Duty Personnel Transaction File	Service Separation Due to Criminal Misconduct	80 to 99

DISCUSSION

Underreporting of personnel security incidents is endemic. DoD personnel security underreporting has long been recognized in anecdotal accounts. This study provides the first objective measurement of the scale of this problem by comparing security issues found in operational DMDC data sources to JPAS incident reports. For all data sources evaluated, the large majority of reportable events were not reported in JPAS, pointing to the systemic failure to comply with personnel security reporting requirements as currently defined in policy.

THE SCALE OF UNDERREPORTING

Despite very liberal criteria for matching events in DMDC data sources to JPAS incident reports, the results of this study demonstrate that non-reporting is the norm. Although reporting rates varied by data source, patterns of underreporting indicate the relative effectiveness (or ineffectiveness) of maintaining reporting requirements for various security concerns. Underreporting may also suggest widespread misconceptions about reporting obligations or the impact of different forms of misconduct on national security.

Sexual Assaults

The estimated underreporting rate for DSAID sexual assaults is 82% to 92%. This is particularly troubling given DoD's sexual assault prevention efforts in recent years. These efforts focused on increased reporting and leadership accountability for military sexual assault. Underreporting rates identified here suggest that work still needs to be done to increase awareness of the need to treat these crimes as personnel security incidents.

Criminal Investigations

Military criminal investigation records from ACRD were among the most frequently reported JPAS incidents. Still, a majority of these records, between 66% and 73%, were not reported. Additionally, the high reporting rate, in comparison to other data sources, is likely due to the longer timeframe covered in this analysis (up to 2 years rather than 6 months).

Positive Drug Tests

The estimated underreporting rate for positive drug test results is 91% to 98%. Unlike other operational data sources included in this study, drug test results data come from a single, well-established DoD program. All positive drug tests are sent directly to the subject's command, and all commanders are responsible for reporting illegal drug use

by their subordinates. These results suggest that military commanders are a critical point of failure in the personnel security reporting system for illegal drug use.

Arrests, Warrants, and Protection Orders

The underreporting rates for validated CE alerts are consistent across data sources analyzed. Nlets arrest underreporting is between 86% and 93%, NCIC warrant underreporting is between 86% and 96%, and NCIC protection order underreporting is between 86% and 95%. The very small number of arrests (n = 687), warrants (n = 118), and protection orders (n = 182) included in this study, compared to other data sources (e.g., 78,484 DCII criminal investigations), reflects the high thresholds for confirming these incidents as new and valid CE alerts. These incidents represent alleged criminal conduct serious enough to merit law enforcement or court action. All of these events are reported to subjects' commands by the CE validation cell. The lack of JPAS reporting for these events, in particular, raises concerns about how SMs, commanders, and supervisors are addressing known security concerns identified via DoD's CE program.

Alcoholism, Drugs, and Criminal Misconduct Service Separations

The estimated underreporting rates for military separations range from 81% to 99% for alcoholism, 65% to 99% for drugs, and 80% to 99% for criminal misconduct. In each case, however, the actual underreporting rate is most likely at the lower end of the range. Unlike the other data sources, the separation event would have to occur *after* the JPAS incident. Separation actions require time for processing, and the triggering incident likely occurred several months prior to separation. In some cases, the triggering incident may have occurred well outside the 6-month time period; for example, a subject sentenced to detention in a military correctional facility will not be separated until completion of the sentence.

Accounting for potential delays, military separations for misconduct are among the least likely events to be underreported. If this is the case, the lower underreporting rate for these events suggests that SMs and commanders may be more likely to create an incident report if the particular event is serious enough to warrant separation. Alternatively, commanders may be more likely to create an incident report if taking a formal personnel security action supports an ongoing separation decision. The disparate underreporting rates for drug-related separations and positive drug tests, as low as 65% compared to 91% to 98%, suggests that commanders are more likely to report after a subject displays a broader pattern of misconduct or poor performance.

LIMITATIONS

Although the scale of underreporting is clearly considerable, it was beyond the scope of this study to identify specific risks to national security that could be associated with underreporting. For example, we did not consider the comparative severity of incidents that were reported or not reported. We were not able to identify risk associated with

any single event or focus on personnel security outcomes (suspensions or revocations) that result from these incident reports. Furthermore, we could not determine whether non-reported incidents were more likely to result in material damage to national security or whether reporting these incidents actually reduced material damage in any identifiable manner. It could not be determined if commanders took action to mitigate unreported security incidents at the local level.

CONCLUSIONS

Underreporting patterns suggest that SMs, commanders, and supervisors may look for definitive "proof" of criminal or substance-abuse-related behavior before inputting this information into JPAS. For example, the apparent increase in reporting rates over time suggests that SMs, commanders, and supervisors may be more likely to create an incident report after an event has resulted in legal action, such as formal investigation, arrest, or prosecution. Further, our findings suggest that SMs are not using adjudicative guidelines properly when creating JPAS incident reports. Specifically, Adjudicative Guideline E: Personal Conduct incident results suggest that this category is used as a catchall for criminal misconduct, which undermines use of more appropriate and specific guidelines. This was particularly evident when considering the relatively high rate of incidents categorized as E: Personal Conduct, rather than J: Criminal Conduct, for separations directly associated with criminal events.

The results clearly show that underreporting is the norm and that known events are not making their way to trained adjudicators for official review and mitigation. This is problematic because adjudication is intended to determine national security eligibility based on a holistic assessment of individuals. By choosing not to record incidents in JPAS, adjudicators are not receiving a complete picture of all relevant information that is, in fact, knowable.

The results of this study also have implications for DoD's continuing efforts to build an effective CE program. As of January 2019, we identified 18 ARCs in active use for those currently enrolled in DoD's CE program. Results of the Mirador analysis show that these alerts are productive, but it is unclear whether SMs are responding to validated alerts and why these alerts are not then recorded as JPAS incidents.

RECOMMENDATIONS

The results of this study raise serious concerns about personnel security reporting practices and the effectiveness of PSP reporting requirements. In this section, we provide a number of practical actions that DoD could take to begin addressing the underreporting rate.

Recommendation 1: Drill down to understand why these serious criminal behaviors go unreported.

Conduct a follow-on study of personnel security reporting to identify why known security concerns are not reported in the field. Focus on the five reportable security events examined in this current effort. This qualitative study, based on interviews with SMs, commanders, supervisors, and other relevant subject matter experts across DoD Components, should address the following research questions:

- How do SM, commander, and supervisor reporting practices differ from reporting requirements established in current policy?
- Do perceptions of an incident's severity influence the likelihood of reporting?
- Do organization security practices, including response to security concerns, influence reporting decisions?
- What cultural norms influence reporting decisions?
- Does JPAS usability impede incident reporting?
- Do SM, commander, and supervisor reporting requirement attitudes and training align with or differ from those of adjudicators?
- Do SMs, commanders, and supervisors have unmet training needs that could improve compliance with reporting requirements?

Recommendation 2: Automate feeds from relevant DoD data sources into JPAS or its successor.

Evaluate the feasibility of automatically creating security incident records in JPAS (or its successor system) from known events recorded in DMDC data sources:

- Review whether it is possible and appropriate to automate processes that would feed DMDC criminal data sources directly into JPAS to establish corresponding incident reports.

Evaluate the feasibility of modifying processes for recording military separations in JPAS to support future adjudication decisions.

- Review current business processes for recording the reason for separation (ISC) in subject JPAS records.
- Develop a process to flag misconduct-related separations in JPAS for review and matching separation to a corresponding incident report.

- Non-derogatory separations should be recorded in JPAS to inform an adjudicator's holistic assessment of the subject in a future personnel security determination.

Recommendation 3: Professionalize the role of SMs in DoD's PSP.

Develop minimum standards for assignment of the SM position across DoD similar to standards applied to adjudicators and background investigators.

Develop a Security Manager's Desk Reference guide to support SM, commander, and supervisor reporting duties and obligations. The objectives of the guide should be to:

- Consolidate personnel security reporting requirements,
- Explain relevance of reportable events to security,
- Distinguish between incident reporting and adjudicative determinations,
- Provide guidance for responding to and mitigating common security concerns, and
- Generate clear instructions for recording information in JPAS.

Recommendation 4: Build an incident report dashboard to provide up-to-date metrics on security incidents.

Develop a data management tool to provide easy-to-access, user-friendly metrics for incident reporting practices. This tool could be used by policy analysts, program stakeholders, and researchers to track and examine:

- The number and type of incident reports recorded;
- Demographic characteristics of reported subjects;
- Characteristics of organizations, including site-specific risk categories;
- Personnel security outcomes associated with incidents; and
- Timeliness of the adjudication process for these issues.

REFERENCES

Department of Defense. (2017a). *DoD Instruction 1010.16: Investigations by DoD Components*. Washington, DC: Author.

Department of Defense. (2017b). *DoD Instruction 6495.02: Sexual Assault Prevention and Response (SAPR) program procedures.* Washington, DC: Author.

Department of Defense. (2017c*). DoD Manual 5200.02: Procedures for the DoD Personnel Security Program (PSP)*. Washington, DC: Author.

Department of Defense. (2018a). *DoD Instruction 1010.01: Military Personnel Drug Abuse Testing Program (MPDATP)*. Washington, DC: Author.

Department of Defense. (2018b). *DoD Instruction 5220.22-R: National Industrial Security Program (NISP)*. Washington, DC: Author.

Department of Defense. (2018c). *DoD Manual 5105.21 (vol. 3): Sensitive Compartmented Information (SCI) administrative security manual: Administration of personnel security, industrial security, and special activities*. Washington, DC: Author.

Department of Defense. (2018d). *DoD Instruction 5505.07: Titling and indexing in criminal investigations*. Washington, DC: Author.

Duncan Hunter National Defense Authorization Act for Fiscal Year 2009. Pub. L. No. 110-417, 122 Stat. 4356 (2008). Retrieved from https://www.govinfo.gov/content/pkg/PLAW-110publ417/pdf/PLAW-110publ417.pdf

Morse, C. G., Baweja, J. A., Prina, D. P., James, K. M., Ortiz, X. B., Gregory, E. R., Munshi, D. C., and Richmond, D. A. (2019). *An evaluation of data sources in DoD's continuous evaluation system*. Seaside, CA: Defense Personnel and Security Research Center.

Nelson, L. C., Beneda, J. G., McGrath, S. M., and Youpa, D. G. (2019). *Enhancing supervisor reporting of events of concern* [TR-19-03]. Seaside, CA: Defense Personnel and Security Research Center.

Office of Management and Budget. (2014). *Suitability and security processes review* [Report to the President]. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf.

Office of the Director of National Intelligence. (2008). *Intelligence Community Policy Guidance Number 704.1: Personnel security investigative standards and procedures governing eligibility for access to Sensitive Compartmented Information and other controlled access program information*. Washington, DC: Author.

Office of the Director of National Intelligence. (2017a). *Security Executive Agent Directive 3: Reporting requirements for personnel with access to classified information or who hold a sensitive position*. Washington, DC: Author.

Office of the Director of National Intelligence. (2017b). *Security Executive Agent Directive 4: National Security Adjudicative Guidelines*. Washington, DC: Author.

Under Secretary of Defense for Personnel and Readiness (USD[P&R]). (2018). *Department of Defense annual report on sexual assault in the military: Fiscal Year 2017*. Washington, DC: Department of Defense.