Standardizing and Automating Security Incident Reporting in the Department of Defense: Feasibility Analysis

Henry Simpson
Northrop Grumman Technical Services

Eric L. Lang
Defense Personnel Security Research Center
Standardizing and Automating Security Incident Reporting in the Department of Defense: Feasibility Analysis

Henry Simpson, Northrop Grumman Technical Services
Eric L. Lang, Defense Personnel Security Research Center

Released By – James A. Riedel

BACKGROUND

The Deputy Undersecretary of Defense for Intelligence (Counterintelligence and Security) (DUSD [CI&S]) oversees information and personnel security programs in Department of Defense (DOD) agencies and industry. Policy will require DOD agencies to submit security incident reports directly to CI&S, where they will be analyzed for patterns and systemic problems perhaps needing policy revisions. Currently, incident reporting varies greatly by agency, and CI&S does not always get the information that it needs. CI&S needs a better method to track and analyze incidents. CI&S tasked PERSEREC to investigate the feasibility of using the Joint Personnel Adjudication System (JPAS) to standardize and automate security incident reporting in the DOD.

HIGHLIGHTS

PERSEREC assessed the feasibility of using JPAS for security incident reporting. The study determined JPAS user information requirements, agency reporting requirements, and developed a notional design of the JPAS reporting capability consisting of a JPAS database, data input screens, and query capability. The study's findings suggest that JPAS reporting is technically feasible, would be acceptable to reporting agencies, and has advantages over the methods currently used to report security incidents. Agencies expressed concerns and raised a number of issues that must be resolved before the feasibility question can be answered definitively. Resolving these issues will require coordination with the DOD user communities affected. The study recommends that CI&S (1) form a working group to coordinate and refine the notional design and resolve related issues, (2) clarify agency reporting requirements, (3) clarify and standardize security incident reporting terminology, and (4) develop a JPAS Reporting Concept of Operations.
PREFACE

The Deputy Undersecretary of Defense for Intelligence (Counterintelligence and Security) (DUSD [CI&S]) is responsible for overseeing information and personnel security programs in Department of Defense (DOD) agencies and industry and has assumed responsibility for tracking and reporting security incidents to the Information Security Oversight Office. Currently, incident reporting varies greatly by agency and DUSD (CI&S) does not always get the information that it needs. DUSD (CI&S) tasked PERSEREC to investigate the feasibility of using of the Joint Personnel Adjudication System (JPAS) for security incident reporting. The concept is for agencies to report their information and personnel security incidents through JPAS and store reports in a JPAS database. This would be a first step toward achieving a DUSD (CI&S) vision of (1) simplifying, automating, expediting, and standardizing incident reporting, (2) facilitating agency-specific analysis and problem-solving, and (3) supporting DUSD (CI&S) efforts to assess and improve security related policies.

This report investigates the feasibility of reporting security incidents through JPAS. It describes the research methodology and presents research findings, agency reactions to the concept, and a set of recommendations.

In May, 2006, PERSEREC concluded the research project and presented results and recommendations to CI&S staff. This report is the formal and complete documentation of that project.

James A. Riedel
Director
ACKNOWLEDGMENTS

The authors greatly appreciate the help of several people who provided guidance, shared professional expertise, and offered opinions, suggestions, and critiques of work in progress. Charleen Wright of the office of the Deputy Under Secretary of Defense (Counterintelligence and Security) outlined the JPAS reporting concept and tasked PERSEREC to perform the work described in this report. Heather Anderson, Chris Baise, Chris Bromwell, and Debbie Ross in the same office shared their ideas and helped us shape the concept.

EXECUTIVE SUMMARY

THE PROBLEM

The Deputy Undersecretary of Defense for Intelligence (Counterintelligence and Security) (DUSD [CI&S]) is responsible for overseeing information and personnel security programs in Department of Defense (DOD) agencies and industry. It has assumed responsibility for tracking and reporting security incidents to the Information Security Oversight Office (ISOO). DOD Regulations 5200.1-R, Information Security Program, (1997) and 5200.2-R, Personnel Security Program (draft), 2002, currently undergoing revision, will require DOD agencies to submit security incident reports directly to DUSD (CI&S), where they will be analyzed for patterns and systemic problems perhaps needing policy revisions. DUSD (CI&S) will also consolidate certain incident report data and forward them to ISOO. Currently, incident reporting varies greatly by agency, and DUSD (CI&S) does not always get the information that it needs. DUSD (CI&S) needs a better method to track and analyze incidents and to support ISOO information requirements. Improvements would also benefit agencies by simplifying, automating, expediting, and standardizing incident reporting, and facilitating agency-specific analysis and problem-solving.

THE REQUIREMENTS

DUSD (CI&S) tasked PERSEREC to investigate the feasibility of using JPAS for security incident reporting. The concept is for agencies to report their security incidents to DUSD (CI&S) through JPAS, where they would be stored in a JPAS database. DUSD (CI&S) would have access scope and authority to the entire database and agencies to their own data. In May, 2006, PERSEREC concluded the research project and presented results and recommendations to CI&S staff. This report is the formal and complete documentation of that project.

OBJECTIVES

The objectives of this project are as follows:

- Assess the feasibility of using JPAS for security incident reporting
- Clarify information and personnel security incident reporting terminology
- Determine user information requirements
- Determine security incident reporting requirements
- Determine agency reactions to JPAS reporting concept
EXECUTIVE SUMMARY

METHODOLOGY

The methodology consists of the following steps:

- **Clarify Terminology.** The terminology associated with security incident reporting is used inconsistently in executive orders and DOD and service policy guidance. To help sort out this lexicon, we reviewed relevant executive orders, DOD directives, and service implementing guidance to locate definitions, determine common usage and where and how key terms are used, and developed operational definitions of key terms for use within the context of security incident reporting.

- **Determine User Information Requirements.** We determined information requirements for users of JPAS incident reporting in DUSD (Cl&S) and reporting agencies by (1) surveying users and reviewing DOD issuances to define DUSD (Cl&S) oversight authority and agency reporting requirements, (2) reviewing current guidance concerning incident reporting and examples of existing reports, and (3) building a set of information requirements based on information and personnel security issuances, investigative frameworks, administrative requirements, suggestions from security experts in DUSD (Cl&S) and agencies, and common sense.

- **Develop Notional Design of JPAS Reporting Capability.** Security incident reporting would be implemented using a JPAS database, data input screens, and query capability. We developed notional designs of a database, data input screens, and query capabilities. Security personnel in reporting agencies would use data input screens to enter security incident report data into the database. Users in DUSD (Cl&S) and reporting agencies would query the database and analyze report data they are authorized to see.

- **Determine Agency Reactions to JPAS Reporting Concept.** We visited DOD agencies to obtain agency reactions to the JPAS reporting concept. We later drafted a paper describing the concept and sent it to agencies requesting their review to help us judge the feasibility of implementing JPAS incident reporting in terms of such issues as impact on agency, any related concerns, and possible use by the agency.

FINDINGS

**Incident Reporting Terminology**

We found so many inconsistencies and ambiguities in security incident reporting terminology that it was necessary to define how the terms are used in this report. The terms at issue are *security violation, security infraction, security incident, compromise, unauthorized disclosure,* and *loss.* One of our recommendations is to develop and publish a standard set of definitions for use by the security community.
User Information Requirements

The JPAS reporting capability would have two sets of users, DUSD (CI&S) and reporting agencies, with DUSD (CI&S) the primary user. We assume that reporting agency information requirements will be a subset of the primary user’s, and may vary among agencies based upon agency interests. Separate sets of information requirements were compiled for information security incidents and personnel security incidents. Both sets of information requirements are structured into four categories:

- Administrative—report number, relevant dates, investigative status, and related information
- Person Reporting Incident—information about the person or persons submitting the report and how to contact them
- Person of Interest—information about the person or persons believed to have been responsible for the incident
- Description of information—description of classified information believed to have been put at risk of compromise

Security Incident Reporting Requirements

Security incident reporting would be implemented using a JPAS database, data input screens, and query capability. Information requirements correspond to fields in the database. Security personnel in reporting agencies would use data input screens to enter security incident report data into the database. Users in DUSD (CI&S) and reporting agencies would query the database and analyze report data to which they have access scope and authority.

Data Input Screens. Notional data input screens were designed to satisfy the information requirements and are based on our analyses, DUSD (CI&S) guidance, and comments from DOD agencies that reviewed a concept paper describing preliminary designs. We made a strong effort to design data input screens that are easy to understand and use.

JPAS does not currently have the capability to report information security incidents. We designed a single screen for reporting information security incidents. JPAS currently has the capability to report personnel security incidents. It is also possible to design an entirely new screen intended for use exclusively by reporting agencies that contains both information and personnel security fields. Doing this would permit agency users to report information and security incidents in the same place.

Query Capability. The JPAS information and personnel security incident database would permit a user to run various types of queries within their access scope and authority. Some possible queries are:
EXECUTIVE SUMMARY

- Find all personnel and information security incident records for a given SSN, name, agency, or agency office
- Determine relative frequency of personnel security incidents based on incident criteria (allegiance to U.S., financial considerations, etc.)
- Determine frequencies of information security incidents by classification levels, information transfer media, or type of information
- Determine frequencies of potential exposures of classified information to unauthorized persons, in the public media, and Sensitive Compartmented Information (SCI) in the public media
- Determine relative frequencies of disclosures of classified information based on probable causes (negligence, willful misconduct, etc.)

Agency Reactions to JPAS Security Incident Reporting Concept

We obtained agency reactions to the JPAS security incident reporting concept by making site visits and obtaining agency comments on a paper describing the concept and including graphic depictions of notional data input screens and their pull-down menus. Agencies accepted the concept without raising objections. Several cited potential benefits, such as that JPAS reporting would:

- Standardize incident reporting across agencies
- Permit DUSD (CI&S) to provide better oversight of information and personnel security programs
- Preclude the need for DOD agencies to report to DUSD (CI&S) directly
- Centralize security incident information in a database that agencies could use to conduct analyses
- Enable agencies to obtain security violation statistics without performing their own labor-intensive data calls
- Provide better visibility to recurrent personnel security incidents involving individuals
- Allow analysis to determine training needs, problem areas, and potential problem employees

Some agency comments expressed underlying concerns that JPAS reporting:

- Might increase workload by requiring duplicate reporting via JPAS and with agency internal incident reporting systems
- Would require agencies to report incidents before investigating them fully and then deciding whether or not to report based on agency criteria
- Might invite DUSD (CI&S) or the CAF receiving the report to become involved in agency decisionmaking
Agencies identified several issues that have practical implications for the successful implementation of JPAS security incident reporting. These include the need to clarify incident reporting terminology, provide user guidance, and assure that reports and the database do not contain classified information. Some agencies objected to including SCI and personnel security information in incident reports.

**Feasibility Assessment**

The study’s findings suggest that JPAS reporting is technically feasible, would be acceptable to reporting agencies, and has clear advantages over the methods currently used to report incidents. At the same time, agencies expressed concerns and raised a number of issues that must be resolved before the feasibility question can be answered definitively. Resolving these issues will require coordination with the DOD user communities affected.

**RECOMMENDATIONS**

**Recommendation 1. Coordinate and Refine Notional Design**

We recommend that DUSD (CI&S) form and chair a working group consisting of subject-matter experts, stakeholders in DUSD (CI&S) and agencies, PERSEREC, and system developers to resolve the remaining issues. DUSD (CI&S) would lead, or designate leadership for, this group. Key issues must be resolved relating to the scope of incident reporting, report and database classification level, and protecting individuals.

**Recommendation 2. Develop a Concept of Operations for JPAS Security Incident Reporting**

A CONOPS is a document that describes the characteristics of a new system from the users’ viewpoint. It can be used to coordinate system definition within the user community and, when finalized, as the basis for developing a Request for Proposal (RFP) or other development-related document.

**Recommendation 3. Clarify and Standardize Incident Reporting Terminology**

We found many inconsistencies and ambiguities in security incident reporting terminology. The DOD security community needs to use terminology consistently to avoid miscommunication and successfully perform its mission. Developing and publishing a standard set of definitions with examples illustrating proper usage of the terms in DOD 5200.1-R, 5200.2-R, and 5200.22-M would facilitate communication and reduce the likelihood of security incident nonreporting and reporting errors.
Recommendation 4. Clarify Agency Reporting Requirements

DOD 5200.1-R requires agencies to report information security incidents to DUSD (CI&S). DOD 5200.2-R does not require agencies to report personnel security incidents to DUSD (CI&S). DUSD (CI&S) should clarify reporting requirements in policy guidance documents.
# TABLE OF CONTENTS

## INTRODUCTION
- THE PROBLEM .......................................................... 1
- THE REQUIREMENTS .................................................. 1

## OBJECTIVES
- ................................................................. 3

## METHODOLOGY
- ................................................................. 4

## FINDINGS
- OVERVIEW .......................................................... 5
- SECURITY INCIDENT REPORTING TERMINOLOGY .................. 5
  - Security Violation .............................................. 6
  - Security Infraction ............................................. 9
  - Security Incident ............................................... 9
  - Compromise, Unauthorized Disclosure, and Loss ................ 10
  - Operational Definitions ....................................... 12
- USER INFORMATION REQUIREMENTS ................................ 12
  - DUSD (CI&S) Oversight Authority .......................... 12
  - Agency Reporting Requirements ............................ 13
  - Information Requirements ................................... 14
- NOTIONAL DESIGN OF JPAS REPORTING CAPABILITY ............... 19
  - Data Input Screens .......................................... 19
  - Linking Information and Personnel Security Incidents ...... 24
  - Query Capability ............................................. 24
- AGENCY REACTIONS TO JPAS SECURITY INCIDENT REPORTING CONCEPT ................................................. 25
  - Acceptability of Concept ................................... 26
  - Agency Concerns ............................................. 26
  - Issues ......................................................... 27

## DISCUSSION AND RECOMMENDATIONS
- FEASIBILITY OF JPAS SECURITY INCIDENT REPORTING ............ 30
  - Recommendation 1. Coordinate and Refine Notional Design .... 30
- SYSTEM DEFINITION ................................................. 31
  - Recommendation 2. Develop Concept of Operations .......... 32
- INCIDENT REPORTING TERMINOLOGY ................................ 32
  - Recommendation 3. Clarify and Standardize Incident Reporting Terminology ........................................ 32
- AGENCY SECURITY INCIDENT REPORTING REQUIREMENTS ........ 32
  - Recommendation 4. Clarify Agency Reporting Requirements 33

## REFERENCES .......................................................... 35

## APPENDIX A CONCEPT PAPER USED IN FIELD SURVEY ............ A-1

## APPENDIX B COMPILATION OF COMMENTS FROM AGENCY VISITS AND FIELD SURVEY ........................................... B-1
TABLE OF CONTENTS

LIST OF TABLES

Table 1   Common Terminology Used in Information and Personnel Security Incident Reporting 7
Table 2   Operation Definitions for Common Terminology Used in Security Incident Reporting 13
Table 3   Information Requirements for Information Security Incident Reporting 16

LIST OF FIGURES

Figure 1  Notional Information Security Incident Data Input Screen 21
Figure 2  Pull-down Menus for Information Security Incident Data Input Screen 22
Figure 3  JPAS Personnel Security Incident Data Input Screen 23
Figure 4  Two Personnel Security Incident Data Input Fields 24
INTRODUCTION
This report investigates the feasibility of reporting security incidents through the use of the Joint Personnel Adjudication System (JPAS). It describes the research methodology and presents research findings, agency reactions to the concept, and a set of recommendations.

THE PROBLEM
The Deputy Undersecretary of Defense for Intelligence (Counterintelligence and Security) is responsible for overseeing information and personnel security programs in Department of Defense (DOD) agencies and industry. It has assumed responsibility for tracking and reporting security incidents to the Information Security Oversight Office (ISOO). DOD Regulations 5200.1-R, Information Security Program (1997) and 5200.2-R, Personnel Security Program (Draft) (2002), will require DOD agencies to submit security incident reports directly to DUSD (CI&S), where they will be analyzed for patterns and systemic problems perhaps needing policy revisions. DUSD (CI&S) will also consolidate certain incident report data and forward them to ISOO. Currently, incident reporting varies greatly by agency, and DUSD (CI&S) does not always get the information that it needs. DUSD (CI&S) needs a better method to track and analyze incidents and to support ISOO information requirements. Improvements would also benefit agencies by simplifying, automating, expediting, and standardizing incident reporting, and facilitating agency-specific analysis and problem-solving.

THE REQUIREMENTS
DUSD (CI&S) tasked PERSEREC to investigate the feasibility of using JPAS for security incident reporting. The DUSD (CI&S) concept is for agencies to report their security incidents to DUSD (CI&S) through JPAS, where they would be stored in a JPAS database. DUSD (CI&S) would have access scope and authority to the entire database and agencies to their own data.

Some potential benefits of JPAS reporting are that JPAS:

- Is already operational and agencies have experience using it
- Could be readily adapted for incident reporting
- Would provide a single, consistent reporting system throughout DOD
- Would simplify and streamline incident reporting
- Would provide a unified historical security incident database
- Would provide new analytical capabilities to DUSD (CI&S) and agencies
INTRODUCTION

- Would retain security data on persons and improve investigations and adjudicative decisions

The first step in defining a JPAS security incident reporting capability is to determine user information requirements. The JPAS reporting capability would have two sets of users: DUSD (CI&S) and reporting agencies. DUSD (CI&S) would be the primary user and its information requirements are key. Reporting agencies would report their incidents to DUSD (CI&S) and might use JPAS to automate paper-based incident reporting, to report and track incidents within the agency, and to analyze agency incident data to which they have authorized access scope and authority. Agencies that rely primarily on paper-based incident reporting might find that JPAS reporting would simplify and streamline their internal incident reporting processes.

DUSD (CI&S) information and personnel security oversight authority is defined in several policy documents and these imply a large potential set of information requirements. DUSD (CI&S) has advised PERSEREC that it intends to use JPAS to oversee only the most essential security incident information, which will be a selected subset of all information that might conceivably be reported. Deciding what information to include and exclude is a judgment call based on scaling criteria such as importance, consequences of nonreporting, suitability for DUSD (CI&S) versus agency oversight, and other factors. A reasonable strategy is to determine the full range of information that might be reportable under current policy, apply scaling criteria to select a recommended information set, and for DUSD (CI&S) then to modify this set based on its own judgment.

The JPAS security incident reporting capability must, above all, satisfy the information requirements of its users and, second, provide tangible benefits to DUSD (CI&S) and reporting agencies. In addition, it is also important that it be easy to learn and use and minimize the burden on reporting agencies.

Implementing DUSD (CI&S)’s security incident reporting concept has several implications beyond the design of the incident reporting capability itself. These include determining required changes to DOD policy, developing a concept of operations, and supporting the software developer, as needed, to develop, test, and evaluate the software and implement it in DOD.
The objectives of this project are as follows:

- Assess the feasibility of using JPAS for security incident reporting
- Clarify information and personnel security incident reporting terminology
- Determine user information requirements
- Determine security incident reporting requirements
- Determine agency reactions to JPAS reporting concept
METHODOLOGY

The methodology consists of the following steps:

- **Clarify Terminology.** The terminology associated with security incident reporting is used inconsistently in executive orders and DOD and service policy guidance. To help sort out this lexicon, we reviewed relevant executive orders, DOD directives, and service implementing guidance to locate definitions, determine common usage and where and how key terms are used, and developed operational definitions of key terms for use within the context of security incident reporting.

- **Determine User Information Requirements.** We determined information requirements for users of JPAS incident reporting in DUSD (CI&S) and reporting agencies by (1) surveying users and reviewing DOD issuances to define DUSD (CI&S) oversight authority and agency reporting requirements, (2) reviewing current guidance concerning incident reporting and examples of existing reports, and (3) building a set of information requirements based on information and personnel security issuances, investigative frameworks, administrative requirements, suggestions from security experts in DUSD (CI&S) and agencies, and common sense.

- **Develop Notional Design of JPAS Reporting Capability.** Security incident reporting would be implemented using a JPAS database, data input screens, and query capability. We developed notional designs of a database, data input screens, and query capabilities. Security personnel in reporting agencies would use data input screens to enter security incident report data into the database. Users in DUSD (CI&S) and reporting agencies would query the database and analyze report data they are authorized to see.

- **Determine Agency Reactions to JPAS Reporting Concept.** We visited DOD agencies to obtain agency reactions to the JPAS reporting concept. We later drafted a paper describing the concept and sent it to agencies requesting their review to help us judge the feasibility of implementing JPAS incident reporting in terms of such issues as impact on agency, any related concerns, and possible use by the agency.
FINDINGS

OVERVIEW
This section begins by reviewing security incident reporting terminology and developing operational definitions of key terms used in that context. It then develops a set of information requirements for users of JPAS incident reporting and describes a notional JPAS security incident reporting capability consisting of a database, data input screens, and query capabilities. The final part summarizes agency reactions to the JPAS reporting concept.

SECURITY INCIDENT REPORTING TERMINOLOGY
The terminology associated with security incident reporting is used inconsistently in executive orders and DOD and service policy guidance. This is a potential source of misunderstanding or confusion. Some terms, such as security violation, have specific definitions that apply within a particular security domain such as information security. However, the definition and usage may change in other security domains, such as personnel, information systems, or physical security. ¹

Terms such as “incident” or “violation” are used both narrowly, in accordance with definitions in policy issuances, and loosely, when following common linguistic conventions. For example, Executive Order (EO) 12958, Classified National Security Information (1995), defines three classes of information security violations, but security practitioners often use the term “violation” generically concerning failure to comply with security rules and regulations. Another example is “incident,” which is used both formally and generically and, in the latter case, has different meanings in information and personnel security domains.

To help sort out this lexicon, we reviewed relevant executive orders, DOD directives, and service implementing guidance to locate definitions, determine common usage and where and how key terms are used. The review included the Department of State Foreign Affairs Manual (FAM) 12 FAM 550, Security Incident Program (2002), because it contains a useful definition separate from the DOD issuances. The following paragraphs discuss key terms, define them where authoritative definitions exist, and highlight possible ambiguities and problems as applicable.

Table 1 summarizes the results. The left-most column divides table rows by security domain (information or personnel), the second column to the right lists issuance, and the remaining columns list six terms widely used in incident reporting (violation, infraction, incident, compromise, unauthorized disclosure, loss). Cells listed below the term row contain any definition (following “def:”) in the

¹ The security domains of concern in this report are information security and personnel security, so the discussion that follows focuses exclusively on them.
issuance or no definition if none appears. Cells also contain information on if and how a term is used following “usage:.” Three different types of usage are (1) blank, if the term is not used; (2) “infosec compromise,” if usage relates to compromise/unauthorized disclosure of classified information; or (3) “persec adj gdlns,” if usage relates to adverse information in the personnel security adjudicative guidelines in EO 12968, Access to Classified Information (1995). A quick scan of the table reveals that many terms are used without definition and that definitions change slightly or have different meanings in different issuances. EO 12968 itself uses “violation” generically concerning failure to comply with security rules and regulations.

Security Violation

**Information Security.** Executive Order 12958 and 13292, Further Amendment to Executive Order 12958, as Amended, Classified National Security Information (2003), contain a clear definition of “violation” that lists three classes of violations: (1) unauthorized disclosure of classified information, (2) improper classification, and (3) improper Special Access Programs (SAP). The definition stipulates that these are “knowing, willful, or negligent action[s].” The same definition appears in DOD 5200.1-R; Army Regulation (AR) 380-5, Department of the Army Information Security Program (2000); and Air Force Instruction (AFI) 31-401, Information Security Program Management (2001); but “violation” is used without definition in Secretary of the Navy Instruction (SECNAVINST) 5510.36, Department of the Navy (DON) Information Security Program (ISP) Regulation (1999), the Navy equivalent of AR 380-5 and AFI 31-401.

“Violation” is not used or defined in DOD Directive (DODD) 5200.1, DOD Information Security Program (1996); or DODD 5220.22, National Industrial Security Program (2004).

**Personnel Security.** None of the personnel security issuances (including EO 12968) defines personnel security violation, and there does not appear to be a personnel security equivalent to the definition of an information security violation. EO 12968 Section 6.2 uses “violation” in a generic sense concerning violations of security regulations. The term “violation” does appear in some of the issuances, but refers to information security violations (paragraph C2.2.1.11) or to various other types of personal or legal matters that reflect individual trustworthiness, reliability, or judgment and fitness for eligibility for a security clearance, for example, allegiance to the U.S. (C2.4.2) and criminal activity (C2.4.3.4).
Table 1  
Common Terminology Used in Information and Personnel Security Incident Reporting

<table>
<thead>
<tr>
<th>Domain</th>
<th>Issuance</th>
<th>Term Description</th>
<th>Issuance</th>
<th>Term Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security</td>
<td>E.O.s 12958 &amp; 13292</td>
<td>def: Any knowing, willful, or negligent action (1) that could reasonably be expected:</td>
<td>E.O.</td>
<td>def: failure to comply with the policy and procedures . . . that reasonably could result in the loss or compromise of classified information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>result in an unauthorized disclosure of classified information, (2) to classify or continue the classification of information contrary to the requirements of this order or its implementing directives, or (3) to create or continue a special access program contrary to the requirements of this order.</td>
<td>12829</td>
<td>def: unauthorized disclosure of classified information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>usage: infosec compromise</td>
<td></td>
<td>usage: infosec compromise</td>
</tr>
<tr>
<td></td>
<td>DoDD 5200.1</td>
<td>def: communication or physical transfer of classified information to an unauthorized recipient</td>
<td></td>
<td>usage: infosec compromise</td>
</tr>
<tr>
<td></td>
<td>DoD 5200.1-R</td>
<td>def: same as E.O. 12958</td>
<td>E.O. 12958</td>
<td>def: unauthorized disclosure of classified information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>agent: same as E.O. 12958</td>
<td></td>
<td>usage: infosec compromise</td>
</tr>
<tr>
<td></td>
<td></td>
<td>usage: infosec compromise</td>
<td></td>
<td>usage: infosec compromise</td>
</tr>
<tr>
<td></td>
<td>E.O. 12829</td>
<td>daf: failure to comply with the policy and procedures . . . that reasonably could result in the loss or compromise of classified information</td>
<td></td>
<td>usage: infosec compromise</td>
</tr>
<tr>
<td></td>
<td>DoDD 5220.22</td>
<td>def: security incident that . . . results in actual or possible compromise of [classified] information</td>
<td></td>
<td>usage: infosec compromise</td>
</tr>
<tr>
<td></td>
<td>DoD 5220.22-M</td>
<td>def: security incident that . . . does not result in actual or possible compromise of [classified] information</td>
<td></td>
<td>usage: infosec compromise</td>
</tr>
<tr>
<td></td>
<td>12 FAM 550</td>
<td>failure to safeguard classified materials</td>
<td></td>
<td>usage: infosec compromise</td>
</tr>
<tr>
<td></td>
<td>AR 380-5</td>
<td>usage: infosec compromise</td>
<td></td>
<td>usage: infosec compromise</td>
</tr>
<tr>
<td></td>
<td></td>
<td>usage: infosec compromise</td>
<td></td>
<td>usage: infosec compromise</td>
</tr>
</tbody>
</table>
### FINDINGS

<table>
<thead>
<tr>
<th>Domain</th>
<th>Issuance</th>
<th>Term</th>
<th>violation</th>
<th>infraction</th>
<th>incident</th>
<th>compromise</th>
<th>unauthorized disclosure</th>
<th>loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECNAVINST 5510.36</td>
<td>usage: infosec compromise</td>
<td>def: same as E.O. 12958</td>
<td>def: infosec compromise</td>
<td>usage: infosec compromise</td>
<td>def: unauthorized disclosure of classified information to a person(s) who do not have a valid clearance, authorized access or a need-to-know</td>
<td>usage: infosec compromise</td>
<td>usage: infosec compromise</td>
<td></td>
</tr>
<tr>
<td>AFI 31-401</td>
<td>def: same as E.O. 12958</td>
<td>security violation or infraction</td>
<td>def: same as E.O. 12958</td>
<td>usage: infosec compromise</td>
<td>usage: infosec compromise</td>
<td>usage: infosec compromise</td>
<td>usage: infosec compromise</td>
<td></td>
</tr>
<tr>
<td>Personnel Security</td>
<td>E.O. 12968</td>
<td>usage: failure to comply with security rules and regulations</td>
<td></td>
<td></td>
<td></td>
<td>usage: persec adj gdlns</td>
<td>usage: persec adj gdlns</td>
<td></td>
</tr>
<tr>
<td>DoDD 5200.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>usage: persec adj gdlns</td>
<td>usage: persec adj gdlns</td>
<td></td>
</tr>
<tr>
<td>DoD 5200.2-R</td>
<td>def: same as E.O. 12958</td>
<td>usage: persec adj gdlns</td>
<td>def: same as E.O. 12958</td>
<td>usage: persec adj gdlns</td>
<td>usage: persec adj gdlns</td>
<td>usage: persec adj gdlns</td>
<td>usage: persec adj gdlns</td>
<td></td>
</tr>
<tr>
<td>E.O. 12829</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>usage: persec adj gdlns</td>
<td>usage: persec adj gdlns</td>
<td></td>
</tr>
<tr>
<td>DoDD 5220.22</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>usage: persec adj gdlns</td>
<td>usage: persec adj gdlns</td>
<td></td>
</tr>
<tr>
<td>DoD 5220.22-M</td>
<td>def: failure to comply with the policy and procedures . . . that reasonably could result in the loss or compromise of classified information</td>
<td>usage: persec adj gdlns</td>
<td></td>
<td></td>
<td></td>
<td>usage: persec adj gdlns</td>
<td>usage: persec adj gdlns</td>
<td></td>
</tr>
<tr>
<td>AR 380-67</td>
<td>usage: persec adj gdlns</td>
<td>usage: persec adj gdlns</td>
<td></td>
<td></td>
<td></td>
<td>usage: persec adj gdlns</td>
<td>usage: persec adj gdlns</td>
<td></td>
</tr>
<tr>
<td>SECNAVINST 5510.30A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>usage: persec adj gdlns</td>
<td>usage: persec adj gdlns</td>
<td></td>
</tr>
<tr>
<td>AFI 31-501</td>
<td>usage: persec adj gdlns</td>
<td>usage: persec adj gdlns</td>
<td></td>
<td></td>
<td></td>
<td>usage: persec adj gdlns</td>
<td>usage: persec adj gdlns</td>
<td></td>
</tr>
</tbody>
</table>

Legend

“infosec compromise” – usage relating to information security compromise/unauthorized disclosure of classified information
“persec adj gdlns” – usage relating to personnel security adverse information in EO 12968 adjudicative guidelines
Security Infraction

**Information Security.** Executive Orders 12958 and 13292 define “infraction” concurrently with “violation” to cover actions contrary to the orders that are not as serious as violations. The definition is given without examples, which leaves it to the reader to decide what qualifies as an infraction. The same definition appears in DOD 5200.1-R, AR 380-5, and AFI 31-401. However, 12 FAM 550 defines the term more narrowly and exclusively in relation to compromise of classified information as “security incident that . . . does not result in actual or possible compromise of [classified] information.” Because of its specificity, it is easier to interpret than the one in the DOD issuances.

**Personnel Security.** DOD 5200.2-R uses the EO 12958/13292 definition in an information security context. “Infraction” is used generically in AR 380-67, Personnel Security Program (1988), and AFI 31-501, Personnel Security Program Management (2005). For an example of such usage, AR 380-67 Appendix E (“Reporting of Nonderogatory Cases”) uses the term in a laundry list of similar ones in scoping significant adverse information in background investigations:

- Incidents, infractions, offenses, charges, citations, arrests, suspicion or allegations of illegal use or abuse of drugs or alcohol, theft or dishonesty, unreliability, irresponsibility, immaturity, instability or recklessness, the use of force, violence or weapons or actions that indicate disregard for the law due to multiplicity of minor infractions.

Security Incident

**Information Security.** “Incident” is not used or defined in the information security executive orders or DOD 5220.22. It is most often used without definition in issuances in a way relating to incidents involving possible compromise of classified information (DOD 5220.22-M, National Industrial Security Program Operating Manual (2006), AR 380-5, SECGNAVIST 5510.36). AFI 31-401 defines it as “security violation or infraction.” 12 FAM 550 defines it specifically as “failure to safeguard classified material.” DOD 5200.1-R does not provide a definition but refers to “incident” in C1.5.3 in a way that includes the three types of violations listed in EO 12958 (unauthorized disclosure of classified information, improper classification, improper SAP). The regulation requires agencies to report all three types of violations to DUSD (CI&S) and it in turn to report them to ISOO. It is not clear to us to what degree agencies understand or meet this requirement. However, our discussions with agency personnel left the impression that they used “incident” to mean an event involving unauthorized disclosure of classified information.

**Personnel Security.** “Incident” is not used or defined in the personnel security executive orders or DODD 5200.2, Department of Defense Personnel Security Program (1999), and is used without definition in other issuances in a way relating to adverse information in the EO 12968 adjudicative guidelines, which includes
possible compromise of classified information, an information security incident. Typical usage is illustrated in the quotation from AR 380-67 presented under the “Security Infraction” heading above.

The issuances use “security incident” in two common and overlapping ways: (1) incidents involving possible compromise of classified information and (2) incidents that raise questions concerning personal trustworthiness based on the adjudicative guidelines. Usage (2) is broader and includes usage (1) in Adjudicative Guideline K, Handling Protected Information.

Compromise, Unauthorized Disclosure, and Loss

“Compromise,” “Unauthorized Disclosure,” and “Loss” are used exclusively in the information security domain. (They do have personnel security implications because a person culpable in such incidents has in all likelihood mishandled protected information and is reportable based on adjudicative guideline K.) The first two terms are used interchangeably in executive orders and DOD and service policy guidance. Executive Orders 12958 and 13292 define “unauthorized disclosure” as “communication or physical transfer of classified information to an unauthorized recipient” and use “compromise” without definition to mean the same thing. DOD 5200.1-R shortens the definition to “unauthorized disclosure of classified information,” not mentioning an information recipient. DOD 5220.22-M uses both terms without definition. The terms are used in context and unlikely to cause confusion. The most important matter is disclosure of classified information. Arguably, the “communication or physical transfer” wording is superfluous inasmuch as it relates to how information is transferred rather than what is transferred.

“Loss” is used in several issuances without definition and usually concurrently with “compromise” or “unauthorized disclosure,” distinguishing it from them. DOD 5200.2 defines loss as “classified information that cannot be physically located or accounted for.”

Probability of Compromise. Compromise of classified information to an unauthorized recipient is the most serious possible outcome of an information security incident. As a practical matter and, depending upon circumstances, the person investigating an incident may judge its consequences to be less serious or unknowable. For example, the applicable military instructions and regulations require that responsible security personnel investigate security incidents and estimate the probability of compromise. Terminology differs slightly, but the probability estimate scale usually includes these categories:

- Certain compromise
- Probable compromise

2 12 FAM 550 Sec 793 paragraph (f) requires reports in the case of incidents involving “loss, theft, abstraction, or destruction,” adding to the lexicon.
• Possible compromise
• No compromise

Attaching such probability estimates in a particular case requires a judgment call based on investigative evidence, circumstances, and the skills and experience of the investigator. The probabilities represented by these terms are not defined in issuances and seem to be based on the investigator’s subjective interpretation. Allowing such discretion is problematical. Picking a term is like using a rating scale. Psychometricians advise rating scale developers to clearly define the construct being rated to maximize validity and reliability (Spector, 1992). It follows that it is important to clearly define exactly what is meant by “certain compromise,” “probable compromise,” and so forth to help investigators decide which term applies. For example, the terms might be translated into statements concerning the probability of compromise as follows: certain (p=100%), probable (50% < p <100%), possible (0% < p ≤ 50%), no (p=0%). Using abstract numeric estimates such as these is difficult and it would be easier to make estimates using more familiar terminology, such as:

• No compromise
• Possible compromise (50% or less chance)
• Probable compromise (more than 50% chance)
• Certain compromise

Alternatively, if policymakers want the terms to be interpreted in some other way, they should so state in policy issuances.

**Damage Assessment.** Damage assessment is an estimate of the possible effects of a security incident upon the national security and, possibly, a security consideration such as command security weaknesses or vulnerabilities in the agency’s information security program revealed by the incident. Logically, it differs from the probability of compromise, although the two different factors (probability of compromise and consequences to national security or possible security vulnerabilities) are sometimes combined.³ Combining the two factors in a single

---

³ For example, SECNAVINST 5510.36 directs authors of preliminary security incident investigative letters to choose one of the following statements in the conclusion of the letter (italics are added to highlight the damage assessment part of the combined statements):

- A loss or compromise of classified information did not occur, but incident meets the criteria of a security discrepancy;
- A loss or compromise of classified information did not occur, however, a security weakness or vulnerability(ies) is revealed due to the failure of a person(s) to comply with established security regulations;
- A loss or compromise of classified information may have occurred but the probability of compromise is remote and the threat to the national security minimal;
FINDINGS

statement confounds them and forces the reporting party to choose the statement that best approximates the available evidence. It is preferable to separate the two factors. One way to present a damage assessment is to use a scale analogous to that described above for probability of compromise:

- No threat to national security
- Possible threat to national security (50% or less chance)
- Probable threat to national security (more than 50% chance)
- Certain threat to national security

It is preferable to assess and report separately other issues revealed by the damage assessment (e.g., command security weaknesses or vulnerabilities in the agency’s information security program).

Operational Definitions

There are so many inconsistencies and ambiguities in security incident reporting terminology that there is a need to define how the terms are used in this report. Table 2 contains operational definitions of terminology based on the issuances reviewed and discussed in this section.

USER INFORMATION REQUIREMENTS

The JPAS reporting capability would have two sets of users, DUSD (CI&S) and reporting agencies, with DUSD (CI&S) the primary user. We assume that reporting agency information requirements will be a subset of the primary user’s, and may vary among agencies based upon agency interests.

DUSD (CI&S) Oversight Authority

DODD 5200.1 defines DUSD (CI&S) information oversight authority and responsibilities and designates DUSD (CI&S) as the senior agency official for the DOD information security program, with the authority to direct, administer, and oversee the program. DODD 5200.2 defines comparable authority and responsibilities for the DOD personnel security program. These two directives put DUSD (CI&S) in charge of the DOD information and personnel security programs, with oversight authority.

- A loss or compromise of classified information may have occurred due to a *significant command security weakness or vulnerability(ies)*; or
- A loss or compromise of classified information occurred, and the *probability of damage to the national security cannot be discounted until after completion of a JAGMAN or NCIS investigation.*
### Table 2
Operation Definitions for Common Terminology Used in Security Incident Reporting

<table>
<thead>
<tr>
<th>Term</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Information Security</strong></td>
</tr>
<tr>
<td>Security Incident</td>
<td>an event that risks the improper disclosure of classified information ^4</td>
</tr>
<tr>
<td>Security Violation</td>
<td>an information security incident that results in possible, probable, or certain compromise of classified information</td>
</tr>
<tr>
<td>Security Infraction</td>
<td>an information security incident that results in no compromise of classified information</td>
</tr>
<tr>
<td>Compromise</td>
<td>unauthorized disclosure of classified information</td>
</tr>
<tr>
<td>Probability of</td>
<td>- no compromise</td>
</tr>
<tr>
<td>Compromise</td>
<td>- possible compromise (50% chance or less)</td>
</tr>
<tr>
<td>Loss</td>
<td>classified information cannot be physically located or accounted for</td>
</tr>
<tr>
<td>Damage Assessment</td>
<td>- no threat to national security</td>
</tr>
<tr>
<td></td>
<td>- possible threat to national security (50% chance or less)</td>
</tr>
<tr>
<td></td>
<td>- probable threat to national security (more than 50% chance)</td>
</tr>
<tr>
<td></td>
<td>- certain threat to national security</td>
</tr>
</tbody>
</table>

### Agency Reporting Requirements

DOD 5200.1-R requires agencies to report information security incidents to DUSD (CI&S), which is required to report them to ISOO. DOD 5200.2-R requires agencies

\^4 This definition reflects the most common usage of “security incident”, and is narrower than usage in DOD 5200.1-R, which is broad enough to encompass the three types of violations listed in EO 12958 (unauthorized disclosure of classified information, improper classification, improper SAP).
to report personnel security incidents to (1) the appropriate Central Adjudication Facility (CAF) for DOD civilian and military personnel or (2) the Defense Industrial Security Clearance Office (DISCO) for contractors. It does not require agencies to report incidents to DUSD (CI&S).5

Information Requirements

From the user’s viewpoint, information requirements are the separate items of information that must be in a database to make it useful. They may be thought of as information fields and may consist of text, categorical information, dates, numbers, and so forth.

A logical starting point in defining information requirements is to review current guidance concerning incident reporting and examples of existing reports. We built sets of information requirements based on information and personnel security issuances, investigative frameworks, administrative requirements, suggestions from security experts in DUSD (CI&S) and agencies, and common sense.

Information Security Incidents. DOD 5200.1-R paragraph C10.1.3. Inquiry/Investigation presents a set of questions that security personnel are directed to address when investigating and reporting information security incidents, such as, “When, where, and how did the incident occur? What persons, situations, or conditions caused or contributed to the incident? Was classified information compromised?” The guidance is quite general but provides a useful framework for conducting an investigation and compiling a report. The military services offer similar but more detailed guidance in AR 380-5, SECNAVINST 5510.36, and AFI 31-401. In addition to these sources, DOD and CIA directives target certain types of classified information of particular and more specialized interest, such as the appearance of classified information in the public media, U.S. intelligence information, and Sensitive Compartmented Information (SCI).

Information requirements can be organized in various ways, for example, with the following four categories:

- Administrative—report number, relevant dates, investigative status, and related information
- Administrative—report number, relevant dates, investigative status, and related information
- Person Reporting Incident—information about the person or persons submitting the report and how to contact them
- Person of Interest—information about the person or persons believed to have been responsible for the incident

5 ISOO Directive 1, Classified National Security Information (1995), requires each agency that creates or handles classified information to report statistics related to its security classification program annually to the Director of ISOO. Note that such statistics concern the agency program and not security incidents.
Description of information—description of classified information believed to have been put at risk of compromise

Table 3 lists the information requirements that we identified in these four categories, five illustrative data types, and related issuances. Data type affects data input ease, speed, likelihood of error, and flexibility, and also has other consequences. The data types described here are useful for illustrative purposes:

- **Text (short)**—short text, typically 64 or fewer characters, as would be used to enter a name, Social Security Number (SSN), and so forth
- **Text (long)**—narrative text, as would be used, for example, to compose an incident description in words. The upper length limit is not yet determined
- **Categorical (yes/no)**—a two-choice category, as would be used to answer a “yes/no” question
- **Categorical (3+)**—a multiple-choice category, as would be used to select one of several different mutually exclusive options from a list
- **Date**—calendar dates of events in numeric format

Executive orders, directives, and instructions listed as Related Issuances target specific types of classified information for the information requirement in the corresponding row. Executive order 12958 covers all types of classified information and so applies to all of these types of information as well.

Shaded cells contain long text blocks that we believe would be primarily of value for reporting agency internal use rather than that of DUSD (CI&S), although DUSD (CI&S) will be able to access them.\(^6\)

The first information requirement under Administrative Information is a report reference number, which must be unique, and that would be assigned automatically by computer. The number would be the report’s identifier and could be used to access the report through query. The remaining administrative information includes a report submission date, incident date, investigative status, and incident closed date. The dates and status information would, among other things, permit a user to determine incident investigative status and how much time elapsed (1) from the occurrence of an incident until it was reported and (2) to investigate and resolve the incident. Looking beyond single incidents, one could construct queries to compare investigative progress across several different reports within an agency or across agencies, or to determine how investigations progressed as a function of other report variables, such as information transfer medium, type of information, and so forth.

---

\(^6\) These blocks are included primarily for internal use by agencies, which typically include such narratives with their incident investigative reports. We assume that DUSD (Cl&S) would not require the length and level of detail provided by such descriptions. Moreover, the long text format is not well suited for compiling queries combining several different incident reports. As noted earlier, user-composed text also poses a greater risk of inadvertently disclosing classified information.
<table>
<thead>
<tr>
<th>Information Category</th>
<th>Information Requirement</th>
<th>Data Type</th>
<th>Related Issuance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative</td>
<td>Report Reference Number</td>
<td>text (short)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Report submission date</td>
<td>date</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incident date</td>
<td>date</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Investigative status</td>
<td>categorical (3+)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Investigation closed date</td>
<td>date</td>
<td></td>
</tr>
<tr>
<td>Person Reporting</td>
<td>Name and title</td>
<td>text (short)</td>
<td></td>
</tr>
<tr>
<td>Incident</td>
<td>Phone</td>
<td>text (short)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Email</td>
<td>text (short)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reporting agency/activity</td>
<td>categorical (3+)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Organization code</td>
<td>text (short)</td>
<td></td>
</tr>
<tr>
<td>Person of Interest</td>
<td>Name</td>
<td>text (short)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SSN</td>
<td>text (short)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Date of birth</td>
<td>date</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Country of birth</td>
<td>categorical (3+)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Citizenship</td>
<td>categorical (3+)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Clearance level</td>
<td>categorical (3+)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SCI access</td>
<td>categorical (yes/no)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SAP access</td>
<td>categorical (yes/no)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Clearance status</td>
<td>categorical (3+)</td>
<td></td>
</tr>
<tr>
<td>Description of</td>
<td>Description of incident</td>
<td>text (long)</td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td>Description of information of concern</td>
<td>text (short)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Classification level</td>
<td>categorical (3+)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information transfer medium</td>
<td>categorical (3+)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Did classified information appear in public media?</td>
<td>categorical (yes/no)</td>
<td>DODD 5210.50 DCID 6/1 (if SCI)</td>
</tr>
<tr>
<td></td>
<td>Was US intelligence information disclosed to foreign parties?</td>
<td>categorical (yes/no)</td>
<td>DCID 6/7 DCID 6/8</td>
</tr>
<tr>
<td></td>
<td>Was SCI information disclosed?</td>
<td>categorical (yes/no)</td>
<td>DCID 6/1</td>
</tr>
<tr>
<td></td>
<td>Was SAP information disclosed?</td>
<td>categorical (yes/no)</td>
<td>DODD 5205.077</td>
</tr>
<tr>
<td></td>
<td>Type of information</td>
<td>categorical (3+)</td>
<td>DODD 6/1 DCID 6/7 DCID 6/8 EO 13292 ISOO Directive 1</td>
</tr>
<tr>
<td></td>
<td>Probability of compromise</td>
<td>categorical (3+)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Damage assessment</td>
<td>categorical (3+)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Probable cause of incident</td>
<td>categorical (3+)</td>
<td></td>
</tr>
</tbody>
</table>

The first three information requirements under *Person Reporting Incident* contain contact information for the person or persons submitting the report. *Reporting agency/activity* is the name of the organization where the incident occurred, such as Army, DFAS, DISCO, and so forth. *Organization code* is a unique code identifying the office submitting the report. It is unclear whether or not there exists a code such as the military’s Universal Identification Code (UIC) that can serve this purpose. If not, one will have to be created. The code serves at least two purposes: (1) uniquely identifies the reporting office and (2) governs whether or not a user in that office or elsewhere will be granted access to the information in the report.

The information requirements under *Person of Interest* all relate to the person or persons believed to have been responsible for the incident and their background, security clearance status, and access to SCI and SAP information. It is possible to have more than one person of interest or for the person of interest to be unknown. Exactly how these contingencies might be handled in practice is not yet determined, but some possibilities are discussed later in this section. The person’s *SSN or Name*, key identifiers, can be used to query the database to find all information (and personnel) security incidents linked to the person whose SSN or name is entered. Other variables such as *Country of birth* and *Citizenship* can also be used to link these variables to other security incidents.

The information requirements under *Description of Information* concern what is believed to have happened during the incident, the type and content of the classified information, classification level, investigative results and conclusions, and corrective actions needed. Each of the requirements is mutually exclusive in the sense that one requirement does not affect any other. *Description of incident*, a narrative telling the story of what happened during the incident, is an exception because it may duplicate information contained elsewhere in *Information Description*. This block was included primarily for internal use by agencies, which typically include a narrative with their incident investigative reports. We assume that DUSD (CI&S) would not require the length and level of detail provided by such a description. Moreover, its narrative format is not well suited for compiling queries combining several different incident reports.

---

8 We distinguish among security clearance status and authority to access SCI or SAP because these are mutually exclusive variables. In practice, SCI or SAP are sometimes treated as clearance levels but EO 12958 Section 1.3 states that information may be classified at one of three classification levels: confidential, secret, or top secret. Further protecting information as SCI or SAP is a separate matter.

9 *Description of incident*, a narrative telling the story of what happened during the incident, is an exception because it may duplicate information contained elsewhere in *Information Description*. This block was included primarily for internal use by agencies, which typically include a narrative with their incident investigative reports. We assume that DUSD (CI&S) would not require the length and level of detail provided by such a description. Moreover, its narrative format is not well suited for compiling queries combining several different incident reports.
FINDINGS

Classification level are self-explanatory. Information transfer medium is the form of information involved, such as paper or other hardcopy; magnetic, optical, or other electromagnetic storage; FAX; or telephone. The next four items all have “yes/no” answers. EO 12958/13292, which covers all forms of classified information, applies in all these situations, but separate DOD and CIA directives target the information covered in some situations.\(^\text{10}\) Type of information uses the eight categories given in EO 13292, such as Foreign government information; Foreign relations or foreign activities of the United States, including confidential sources; Military plans, weapons, or operations; and so forth. Probability of compromise and Damage assessment are estimates, as described earlier under the subsections with these titles. Probable cause of incident is a judgment concerning why the incident occurred, such as negligence or willful misconduct. Mitigating circumstances should be self-explanatory. Corrective actions.... and Further actions required are narratives describing what actions have been taken and will be taken. As with Description of incident, we believe that these narratives will be more important to agencies than to DUSD (CI&S).

**Personnel Security Incidents.** DOD 5200.2-R paragraph C9.1.2.1 requires agencies to refer for action any “derogatory information [that] is developed or otherwise becomes available” relating to the trustworthiness of a person to preserve the national security. This guidance is presented in the context of a regulation that frames trustworthiness in terms of the adjudicative guidelines.

Like information security incidents, personnel security incidents must be investigated and have similar information requirements. The first three categories—Administrative, Person Reporting Incident, Person of Interest—are identical to those for information security incidents, although the specific information requirements in each category may differ in importance. The last category, Information Description, translates for personnel security incidents as Incident Description. The Incident Description consists of two information requirements:

1. Description of incident—a narrative description of the incident (text [long] data type)
2. Adjudicative guideline— which of the adjudicative guidelines is applicable (categorical [3+] data type)

\(^{10}\) DODD 5210.50, Unauthorized Disclosure of Classified Information to the Public (July 22, 2005) and Director of Central Intelligence Directive (DCID) 6/1, Security Policy for Sensitive Compartmented Information (1995) both concern the appearance of classified information in public media. DCID 6/7, Intelligence Disclosure Policy (2001) and DCID 6/8, Unauthorized Disclosures, Security Violations, and Other Compromises of Intelligence Information (2002) concern the disclosure of U.S. intelligence information to foreign parties.
NOTIONAL DESIGN OF JPAS REPORTING CAPABILITY

Security incident reporting would be implemented using a JPAS database, data input screens, and query capability. Information requirements, discussed earlier, correspond to the fields in the database. Security personnel in reporting agencies would use data input screens to enter security incident report data into the database. Users in DUSD (CI&S) and reporting agencies would query the database and analyze report data to which they have access scope and authority.

Data Input Screens

Notional data input screens were designed to satisfy the information requirements described in the previous section. The designs are based on our own analyses, DUSD (CI&S) guidance, and comments from DOD agencies that reviewed a concept paper that described the screens.11

Agencies expressed some concern about the possible impact of JPAS on agency reporting workload, and this makes it particularly important to provide data input screens that are easy to understand and use. We earlier noted that data type affects data input ease, speed, likelihood of error, and flexibility, and also has other consequences. In general, categorical information has advantages over text in terms of speed and accuracy of data input via menus, check boxes, and other data input methods that allow the user to select rather than have to recall and correctly type in and spell the required input. Categorical information must fall into predictable and unambiguous categories. Some types of data do not meet these requirements. Examples are names, Social Security Numbers (SSN), narrative descriptions, and the like. The advantages of categorical information also apply during query, for they permit users to query by selecting rather than typing in the query criteria.

Some other commonsense ways to facilitate data input are to:

- Structure the screen in terms of its information categories (Administrative Information, Person Reporting Incident, etc.) and subcategories (input fields in each category)
- Clearly title information categories and provide clear prompts for each data input field
- Align data input fields vertically so that, as the user enters data, the cursor moves down the screen to the next field in a logical fashion.
- Provide online help

Information Security Data input Screen. JPAS does not currently have the capability to report information security incidents. Figure 1 illustrates a notional information security incident data input screen based on the information

---

11 DOD agencies commented on several aspects of the JPAS reporting concept in addition to the data input screens. Their comments are discussed in greater detail later under the heading Agency Reactions to JPAS Security Incident Reporting Concept.
requirements in Table 3. As envisioned here, the screen is structured to collect four categories of information: Administrative Information, Person Reporting Incident, Person of Interest, Description of Information. The first field, Reference Number, is assigned automatically and the remaining fields are entered as text or selected as categorical options via check boxes or pull-down menus. Figure 2 illustrates the contents of the menus. Menu content is based on our best estimate of the type of information required in each of these fields based on policy issuances and inputs from DUSD (CI&S) and agencies that commented on the preliminary design.

We noted earlier that there may be more than one person of interest. It is also possible that other data input fields may require more than a single entry. If this is the case, then the data input screen must be adapted to permit multiple entries. Another possibility is to provide the additional information in a report attachment or in some other way. Analogous procedures must be established to handle cases where the person of interest is unknown, for example, by entering “unknown” in the Name field or simply leaving fields blank.
Information Security Incident Report

### Administrative Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report reference no.</td>
<td></td>
</tr>
<tr>
<td>Report submission date</td>
<td></td>
</tr>
<tr>
<td>Incident date</td>
<td></td>
</tr>
<tr>
<td>Incident investigative status</td>
<td>□ Ongoing</td>
</tr>
<tr>
<td></td>
<td>□ Closed [date]</td>
</tr>
</tbody>
</table>

### Person Reporting Incident

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name and title</td>
<td></td>
</tr>
<tr>
<td>Phone</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td></td>
</tr>
<tr>
<td>Reporting agency/activity</td>
<td>▼ menu 1</td>
</tr>
<tr>
<td>Organization Code</td>
<td></td>
</tr>
</tbody>
</table>

### Person of Interest

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>SSN</td>
<td></td>
</tr>
<tr>
<td>Date of birth</td>
<td></td>
</tr>
<tr>
<td>Country of birth</td>
<td>▼ menu 2</td>
</tr>
<tr>
<td>Citizenship</td>
<td>▼ menu 3</td>
</tr>
<tr>
<td>Clearance Level</td>
<td>▼ menu 4</td>
</tr>
<tr>
<td>Check all that apply</td>
<td>□ SCI access</td>
</tr>
<tr>
<td></td>
<td>□ SAP access</td>
</tr>
<tr>
<td>Clearance status</td>
<td>▼ menu 5</td>
</tr>
</tbody>
</table>

### Description of Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Describe incident (unclassified)</td>
<td></td>
</tr>
<tr>
<td>Describe information of concern (unclassified)</td>
<td></td>
</tr>
<tr>
<td>Classification level</td>
<td>▼ menu 6</td>
</tr>
<tr>
<td>Information transfer medium</td>
<td>▼ menu 7</td>
</tr>
<tr>
<td>Check all that may apply</td>
<td>□ Classified information in public media</td>
</tr>
<tr>
<td></td>
<td>□ US intelligence information to foreign parties</td>
</tr>
<tr>
<td></td>
<td>□ SCI information</td>
</tr>
<tr>
<td></td>
<td>□ SAP information</td>
</tr>
<tr>
<td>Type of information</td>
<td>▼ menu 8</td>
</tr>
<tr>
<td>Probability of compromise</td>
<td>▼ menu 9</td>
</tr>
<tr>
<td>Damage assessment</td>
<td>▼ menu 10</td>
</tr>
<tr>
<td>Probable cause of incident</td>
<td>▼ menu 11</td>
</tr>
<tr>
<td>Mitigating circumstances</td>
<td></td>
</tr>
<tr>
<td>Corrective actions taken</td>
<td></td>
</tr>
<tr>
<td>Further actions required</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 1** Notional Information Security Incident Data Input Screen
Figure 2  Pull-down Menus for Information Security Incident Data Input Screen

Personnel Security Data Input Screen. JPAS currently has the capability to report personnel security incidents using the data input screen illustrated in Figure 3. It would be possible to design an entirely new screen that contains both information and personnel security fields. Doing this would permit agency users to report information and security incidents in the same place. (One agency recommended to “combine the personnel and information security incident screens
so that information is reported in a consistent manner.”) Such a screen might be envisioned as Figure 1 with two additional fields for *Description of incident* and *Adjudicative guideline*. Figure 4 shows how these two fields might appear by themselves before being grafted onto the Information Security Incident Reporting Screen (Figure 1). Information and personnel security incidents are sometimes linked (see below) and being able to report them in the same place would eliminate the need for routing between two different data input screens.

Personnel Security Incident Report

<table>
<thead>
<tr>
<th>[Person of Interest Name]</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SSN:</td>
<td>Date of Birth:</td>
</tr>
<tr>
<td>Eligibility:</td>
<td>Place of Birth:</td>
</tr>
<tr>
<td>Investigation:</td>
<td>Citizenship:</td>
</tr>
<tr>
<td>Open Investigation:</td>
<td></td>
</tr>
<tr>
<td>Incident Report:</td>
<td></td>
</tr>
<tr>
<td>Polygraph:</td>
<td></td>
</tr>
<tr>
<td>Foreign Relation:</td>
<td>▼ menu</td>
</tr>
</tbody>
</table>

Select an Existing Incident: ▼ menu

Incident Status □ Initial □ Follow-up □ Final

Date of Incident:               Suspension Start Date:  

Action: □ Suspend Access  

Select CAF: ▼ menu

Incident Criteria:

- □ Allegiance to the United States
- □ Foreign Influence
- □ Foreign Preference
- □ Sexual Behavior
- □ Personal Conduct
- □ Financial Considerations
- □ Alcohol Consumption
- □ Drug Involvement
- □ Emotional, Mental and Personality Disorders
- □ Misuse of Information Technology Systems
- □ Security Violations
- □ Outside Activities
- □ Criminal Conduct

Incident Report

<table>
<thead>
<tr>
<th>Status</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
</table>

Unclassified Description of Incident:

Figure 3  JPAS Personnel Security Incident Data Input Screen
FINDINGS

<table>
<thead>
<tr>
<th>Unclassified Description of Personnel Security Incident:</th>
<th>Adjudicative guideline:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>□ Allegiance to the United States</td>
</tr>
<tr>
<td></td>
<td>□ Foreign Influence</td>
</tr>
<tr>
<td></td>
<td>□ Foreign Preference</td>
</tr>
<tr>
<td></td>
<td>□ Sexual Behavior</td>
</tr>
<tr>
<td></td>
<td>□ Personal Conduct</td>
</tr>
<tr>
<td></td>
<td>□ Financial Considerations</td>
</tr>
<tr>
<td></td>
<td>□ Alcohol Consumption</td>
</tr>
<tr>
<td></td>
<td>□ Drug Involvement</td>
</tr>
<tr>
<td></td>
<td>□ Psychological Conditions</td>
</tr>
<tr>
<td></td>
<td>□ Criminal Conduct</td>
</tr>
<tr>
<td></td>
<td>□ Handling Protected Information</td>
</tr>
<tr>
<td></td>
<td>□ Outside Activities</td>
</tr>
<tr>
<td></td>
<td>□ Misuse of Information Technology Systems</td>
</tr>
</tbody>
</table>

Figure 4  Two Personnel Security Incident Data Input Fields

We lack sufficient information about the relative costs and benefits of these two alternatives to recommend which one (or perhaps another altogether) to pursue. The least expensive solution in terms of development cost is to use the current personnel screen (Figure 3). Alternatively, being able to use one screen to input both types of incidents would probably have additional benefits in terms of ease and speed of data input.

Linking Information and Personnel Security Incidents

Personnel security incidents and information security incidents may be linked if one type of incident suggests that the other has also occurred. For example, a personnel security incident involving mishandling of protected information (Adjudicative Guideline K) is also reportable as an information security incident. Information security incidents may indicate the reverse of this situation if a person holding a security clearance is responsible for an event that risks the improper disclosure of classified information.

In cases where both types of incident reports are applicable, the user creating the first report should know that the second is also required. However, rather than relying on the user, JPAS could use software logic to detect such requirements, alert the user, and automatically transfer any redundant information (name, SSN, date of birth, citizenship, etc.) to the second report to preclude having to enter it twice.\(^\text{12}\)

Query Capability

The JPAS information and personnel security incident database would permit a user to run various types of queries within their access scope and authority. Some possible queries are:

\(^{12}\) An alternative is to combine personnel and information security incident screens so that both types of incidents would be reported in the same place, as described earlier.
• Find all personnel and information security incident records for a given SSN, name, agency, or agency office
• Determine relative frequency of personnel security incidents based on incident criteria (allegiance to U.S., financial considerations, etc.)
• Determine frequencies of information security incidents by classification levels, information transfer media, or type of information
• Determine frequencies of potential exposures of classified information to unauthorized persons, in the public media, and SCI in the public media
• Determine relative frequencies of disclosures of classified information based on probable causes (negligence, willful misconduct, etc.)

The database permits many different types of queries, but several questions need to be answered before designing the query capability, for example:
• What types of queries would be of value to users?
• How do user query preferences vary among different users?
• What are user preferences for fixed versus user-defined queries?
• How much flexibility should users have to construct their own queries?
• What type of user interface should be provided?
• How would access scope and authorities be defined, assigned, managed, and controlled?

Answering these and related questions is beyond the scope of the present report. If a decision is made to implement the JPAS security incident reporting concept, the questions should be addressed during system definition.13

AGENCY REACTIONS TO JPAS SECURITY INCIDENT REPORTING CONCEPT

We visited three agencies at the outset of the project to explain the JPAS incident reporting concept and solicit agency reactions. The visits were made before we had conducted the analyses described in Methodology to clarify terminology, determine user information requirements, or determine security incident reporting requirements. We later drafted a six-page paper (Appendix A) describing the concept that included illustrations of notional data input screens and their menus. We sent an email with the concept paper as an attachment to representatives in 12 different DOD agencies and activities, including the three that participated in our initial site visits.14 The email requested recipients to review the paper to help us

13 System Definition is discussed in greater detail in Discussion and Recommendations.
14 Agencies and activities participating in site visits and/or the field survey include the Office of the Deputy Chief of Staff (Intelligence), Army; Defense Contract Management Agency; Defense Industrial Security Clearance Office; Defense Logistics Agency;
judge the feasibility and desirability of implementing JPAS incident reporting in terms of such issues as impact on agency, any related concerns, and possible use by the agency, and to send PERSEREC their suggestions and recommendations. Eight agencies responded to the field survey. In most cases, the agency response was drafted by a single person who consolidated comments of several agency reviewers. The comments are summarized below under three broad headings: Acceptability of Concept, Agency Concerns, and Issues. Appendix B, Compilation of Comments from Agency Visits and Field Survey, presents the comments in complete and raw form as we recorded them during discussions and as they were sent to us via email. The comments are slightly edited for clarity, coded 1-8 based on responding agency, and clustered into subject areas. They do not include technical comments relating to design (e.g., contents of a pull-down menu), although those comments were taken into account in designing the JPAS reporting capability.

Acceptability of Concept

Agencies accepted the concept without raising objections. Several cited potential benefits, such as that JPAS reporting would:

- Standardize incident reporting across agencies
- Permit DUSD (CI&S) to provide better oversight of information and personnel security programs
- Preclude the need for DOD agencies to report to DUSD (CI&S) directly
- Centralize security incident information in a database that agencies could use to conduct analyses
- Enable agencies to obtain security violation statistics without performing their own labor-intensive data calls
- Provide better visibility to recurrent personnel security incidents involving individuals
- Allow analysis to determine training needs, problem areas, and potential problem employees

Agency Concerns

Although agencies accepted the JPAS reporting concept in the abstract, some of their comments, summarized briefly below, expressed underlying concerns. Because of the small number of respondents, we cannot say how widely these concerns are shared.

Additional Reporting Burden. Agencies expressed concern that JPAS reporting might increase their workload by requiring duplicate reporting via JPAS and with their own internal incident reporting systems. A parallel concern is that
agencies would be required to report SCI-related incidents to DUSD (CI&S) in addition to reporting them to the Director of National Intelligence (DNI).

**Usurpation of Agency Prerogatives.** This concern seems to reflect a perception that JPAS reporting would require agencies to report incidents before investigating them fully and then deciding whether or not to report based on agency criteria. For example, agencies may believe it unnecessary to report information security incidents not yet determined to have resulted in compromise or been caused by knowing, willful, or negligent action; or personnel security incidents that have not yet been found to have a valid basis. In this connection, one respondent commented, “If a report is entered prematurely, the ‘person of interest’ may be inappropriately branded with derogatory information before [his or her] guilt has been determined.” Another said that, “non-compromise incidents do not have to be reported in JPAS.”

Agencies may also perceive that preinvestigative incident reporting might invite DUSD (CI&S) or the CAF receiving the report to “get involved in local decision-making . . . that was previously done in [the agency],” as one respondent stated. He went on to suggest that there might be a way to report data and not have the recipient take immediate action on it, perhaps by establishing rules that define what should trigger action.

Agencies may feel that it is their prerogative to decide what and when to report. Whether or not this is proper, other comments suggested that agencies lacked a common understanding of what was or should be reportable as a security incident and at what point in time. (This relates to an issue discussed below, namely, the need to provide users with adequate guidance.)

**Issues**

Agencies identified several issues that have practical implications for the successful implementation of JPAS security incident reporting. These include the need to clarify incident reporting terminology, provide user guidance, and assure that reports and the database do not contain classified information. Some agencies objected to including SCI and personnel security information in incident reports.

**Clarify Terminology.** Several agency comments reinforced our conclusion that the terminology associated with security incident reporting is a potential source of misunderstanding or confusion. One respondent stated, “violation, incident’ terminology needs careful definition,” another recommended that the concept paper should “include widely recognized definitions for terms,” and a third declared that “incident” [was usually used] in relation to information security and ‘violation’ for personnel security.” Comments such as these suggest that respondents recognized the need to define and use terminology carefully.
**FINDINGS**

**Provide User Guidance.** Agencies expressed the need for user guidance to support the use of JPAS security incident reporting. The type of guidance mentioned includes:

- Agency requirements to report incidents to DOD
- Definition of what events or circumstances require an incident report
- When, in relation to the investigative process, reports must be submitted
- Who is authorized to submit incident reports
- A classification guide to support incident reporting
- Updated DOD 5200.1-R and 5200.2-R

**Report and Database Classification Level.** DUSD (Cl&S) has advised us that JPAS security incident reporting is intended to operate at the unclassified level. Some agencies expressed concern about the risk that JPAS users might inadvertently enter classified information in their reports, enter separate items of unclassified information that, when combined, revealed something classified, or that the incident database itself might become classified. One agency commented as follows about the information security incident data input screen:

> There is too much information/details on the information security incident to be placed on an unclassified system. If all menus are completed on the unclassified system, and it ever gets hacked into, I could find out that the Army had a S/SCI document, with the description of the information, placed on the SIPRNET. [This agency] has no problem with including menus 1, 5, 6, 9, and 10, but we need to be very careful with menus 7 and 8. In the SCI arena, if there has been a compromise of classified information in the media, DIA would like the report to be at least CONFIDENTIAL. This would eliminate the ability to add the information into JPAS.

A related consideration is the scope and amount of information included in incident reports. The concept paper describes a notional system for both personnel and information security incidents, with the information security incidents to include those involving SCI, SAP, and intelligence-related information. One way to reduce the risk of creating a classified report or database is to reduce what must be reported in terms of the type of information and how it is described in the report. The risk of creating a classified report would seem to increase with the

---

15 Comments were made in the context of a proposed new system, but some suggest that agencies believe that they lack adequate guidance in how they currently report security incidents.

16 The menus referred to are equivalent to those shown in Figure 2. Menus 7 and 8, which the respondent objects to, contain information concerning *Information Transfer Medium* and *Type of Information*. 
classification level of the information involved in the security incident itself and the
degree to which the report contains text-based rather than categorical information.

Inadvertent entry of classified information can be minimized by training,
experience, and review of reports prior to submission. Another way to reduce the
danger is to provide adequate user guidance (see above). However, the danger
remains.

**Inclusion of SCI-Related Information.** As noted earlier, agencies expressed
concern that JPAS reporting might increase their workload by requiring them to
report SCI-related incidents to DUSD (CI&S) in addition to DNI. One agency’s
response recommended at considerable length against reporting SCI-related
incidents in JPAS on the basis both of added workload and procedural
considerations such as the requirement that “security violations involving SCI be
reported to DIA/DAC-3D within 72 hours.”

**Reporting of Personnel Security Incidents in JPAS.** As noted, agencies
commented both on the possible benefits of reporting personnel security incidents
in JPAS (e.g., it would increase visibility of recurrent incidents for individuals) and
drawbacks (e.g., prematurely tagging an individual as at-risk, inviting DUSD (CI&S)
or CAF involvement in local decisionmaking). One agency argued against reporting
such incidents in JPAS, as follows:

Most personnel security-related incidents are dealt with via PSI and
adjudication, for which JPAS has, or is developing, tools sufficient to
DUSD(I) reportage . . . Consequently, I see no need to go beyond
[information security] incident reporting . . .
DISCUSSION AND RECOMMENDATIONS

The study described in this report was conducted to investigate the feasibility of using JPAS for security incident reporting in DOD. The first subsection discusses feasibility, the need to coordinate and refine the notional design, and some related issues that need to be addressed. The next subsection discusses system definition and the need for a Concept of Operations (CONOPS) for JPAS security incident reporting. The third and fourth subsections discuss and present recommendations relating to two issues identified during the study that are important to security incident reporting whether done with JPAS or by traditional methods: clarifying and standardizing terminology and clarifying agency reporting requirements.

FEASIBILITY OF JPAS SECURITY INCIDENT REPORTING

The study’s findings suggest that JPAS reporting is technically feasible, would be acceptable to reporting agencies, and has clear advantages over the methods currently used to report incidents. At the same time, agencies expressed concerns and raised a number of issues that must be resolved before the feasibility question can be answered definitively. Resolving these issues will require coordination with the DOD user communities affected.

Recommendation 1. Coordinate and Refine Notional Design

We recommend that DUSD (CI&S) form and chair a working group consisting of subject-matter experts, stakeholders in DUSD (CI&S) and agencies, PERSEREC, and system developers to resolve the remaining issues. DUSD (CI&S) would lead, or designate leadership for, this group. The issues are described below.

Issue 1: Determine the Scope of Incident Reporting. This report describes a notional design based on an enormous potential set of personnel and information security information requirements. DUSD (CI&S) has indicated that it intends to use JPAS to oversee only the most essential security incident information, which must be selected from the potential set of requirements. We have not attempted to prioritize or prejudge what requirements to include. This task is best left to policymakers in DUSD (CI&S) in coordination with agencies and other parties designated by DUSD (CI&S).

Issue 2: Report and Database Classification Level. DUSD (CI&S) has advised us that JPAS security incident reporting is intended to operate at the unclassified level. Some agencies expressed concern about the risk that JPAS users might inadvertently enter classified information in their reports, enter separate items of unclassified information that, when combined, revealed something classified, or that the incident database itself might become classified. This is a
valid concern and there appear to be two obvious ways to address it. The first is to operate the system at the classified level, reversing DUSD (CI&S)’s expressed intention to us. The second is to limit the scope and amount of information included in incident reports to minimize the risk of classification. If the second alternative is to be followed, then expert judgment must be exercised to decide how, exactly, to “limit the scope and amount of information to include.”

**Issue 3: Inclusion of Intelligence-Related Information.** Agencies expressed concern that JPAS reporting might require them to report SCI-related incidents to DUSD (CI&S) in addition to DNI. This concern relates to possible increases in workload and, more importantly, to a requirement to report to DUSD (CI&S) incidents that are in the jurisdiction of DNI. This concern can be generalized to all intelligence-related incidents currently reportable to DNI. Requiring agencies to report such information to DUSD (CI&S) increases the risk of report and database classification and creates an additional reporting burden on agencies. Policymakers in DUSD (CI&S) must decide if the potential benefits of such reporting outweigh the risks, impact on agencies, and costs.

**Issue 4: Protecting Individuals.** Agencies recognized the benefits of reporting personnel security incidents in JPAS but were concerned about the risks to individual reputations of immediately reporting personnel security incidents not yet fully investigated and found to have a valid basis. One way to limit risk is to establish policy and operating procedures that control how information on individuals is reported, processed, and resolved so that individuals are protected. Moreover, this effort must address the privacy issues, rights of notification, review, challenge, and appeal of failed challenges to information stored individuals. Permissible uses need to be defined beyond simple general use by DUSD (CI&S) of all data and agencies’ use of their own data. Rational and fair data retention schedules also need to be developed.

**SYSTEM DEFINITION**

The notional design described in this report includes a database, data input screens, and query capabilities. It also addresses the need to define logic rules governing data access scope and authority for users and link information and personnel security incident reporting. It left many questions unanswered. These include whether personnel security incidents would be reported using the existing JPAS screen or with an entirely new screen and whether incident reporting should be expanded beyond incidents of possible compromise to include those of improper classification or SAP. If a decision is made to implement the JPAS reporting concept, then the JPAS reporting “system” needs to be defined in greater detail.

---

17 A third possibility is to compartmentalize the database into unclassified and classified parts.
DISCUSSION AND RECOMMENDATIONS

Recommendation 2. Develop Concept of Operations

A CONOPS is a document that describes the characteristics of a new system from the users’ viewpoint. IEEE Standard 1362-199818 (IEEE Standards Association, 1998) is the common standard describing what goes in a CONOPS. The contents and uses of a CONOPS are described in the standard’s abstract as follows:

The ConOps document is used to communicate overall quantitative and qualitative system characteristics to the user, buyer, developer, and other organizational elements (for example, training, facilities, staffing, and maintenance). It is used to describe the user organization(s), mission(s), and organizational objectives from an integrated systems point of view.

Significantly, the CONOPS places the technical attributes of the system (database, data input screens, and so forth) within the larger context of a total “system” comprising organizational elements, and other parties with various roles in relation to the system. A CONOPS can be used to coordinate system definition within the user community and, when finalized, used as the basis for developing a Request for Proposal (RFP) or other development-related document.

INCIDENT REPORTING TERMINOLOGY

We found many inconsistencies and ambiguities in security incident reporting terminology and felt it necessary to create operational definitions of the terms for use in this report. Agency comments echoed our findings. The DOD security community needs to use terminology consistently to avoid miscommunication and successfully perform its mission. Some terms lack published definitions, have more than one definition, or are used in ways at variance with published definitions.

Recommendation 3. Clarify and Standardize Incident Reporting Terminology

Developing and publishing a standard set of definitions with examples illustrating proper usage of the terms in DOD 5200.1-R, 5200.2-R, and 5200.22-M would facilitate communication and reduce the likelihood of security incident nonreporting and reporting errors. The suggested definitions in Table 2 are a possible starting point for such definitions.

AGENCY SECURITY INCIDENT REPORTING REQUIREMENTS

DOD 5200.1-R requires agencies to report information security incidents to DUSD (CI&S). DOD 5200.2-R does not require agencies to report personnel security incidents to DUSD (CI&S).

18 The elements of a CONOPS are described at this URL: http://standards.ieee.org/reading/ieee/std_public/description/se/1362-1998_desc.html
Recommendation 4. Clarify Agency Reporting Requirements

If DUSD (CI&S) wants agencies to submit personnel security incident reports to it directly, or to have their current recipients forward them, it should establish the requirement in policy guidance such as DOD 5200.2-R. Agency comments reinforced our conclusion about the need to clarify incident reporting requirements.
REFERENCES


Director of Central Intelligence Directive 6/8, Unauthorized Disclosures, Security Violations, and Other Compromises of Intelligence Information, December 9, 2002.
REFERENCES


Executive Order 13292, Further Amendment to Executive Order 12958, as Amended, Classified National Security Information, March 25, 2003.


Secretary of the Navy Instruction 5510.36, Department of the Navy (DON) Information Security Program (ISP) Regulation, March 17, 1999.

APPENDIX A

CONCEPT PAPER USED IN FIELD SURVEY
Concept Paper: JPAS Security Violations Reporting

This paper describes a security incident reporting concept that PERSEREC is developing for the office of the Deputy Undersecretary of Defense for Intelligence (Counterintelligence and Security). The first section describes DUSD(CI&S) oversight and security incident reporting responsibilities and some shortcomings of the current incident reporting process. The second section describes the proposed system, potential benefits, guiding principles, notional data input screens, and some queries that DUSD(CI&S) or agencies might run. The last section solicits your agency’s comments and suggestions about the concept.

Background

DUSD(CI&S) is responsible for overseeing information and personnel security programs in DOD agencies and industry. It has assumed responsibility for tracking and reporting security incidents to the Information Security Oversight Office (ISOO). DOD Directives 5200.1-R and 5200.2-R, currently undergoing revision, will require DOD agencies to submit security incident reports directly to DUSD(CI&S), where they will be analyzed for patterns and systemic problems perhaps needing policy revisions. DUSD(CI&S) will also consolidate certain incident report data and forward it to ISOO. Currently, incident reporting varies greatly by agency, and DUSD(CI&S) does not always get the information that it needs. DUSD(CI&S) needs a better method to track and analyze incidents and to support ISOO information requirements. Improvements would also benefit agencies by simplifying and standardizing incident reporting and automating incident reporting and analysis.

Proposal

In a nutshell, what is proposed is for agencies to report their security incidents to DUSD(CI&S) through JPAS, where they would be stored in a JPAS database. Incidents would be reported at the unclassified level. DUSD(CI&S) would have access to the entire database and agencies to their own data (but not to data reported by other agencies).

JPAS reporting has several potential benefits. Perhaps the most obvious is that DOD agencies already know and use it. Others are that JPAS:

- Is fielded and could be readily adapted for incident reporting
- Would provide a single, consistent reporting system throughout DOD
- Would simplify and streamline incident reporting
- Would provide a unified historical security incident database
- Would provide new analytical capabilities to DUSD(CI&S) and agencies
- Would retain security data on persons improving investigations and adjudicative decisions
The JPAS security incident reporting concept is being developed according to several guiding principles:

- Focus exclusively on (1) information security incidents involving possible or probable or confirmed compromise of classified information and (2) personnel security trustworthiness incidents
- Minimize the burden on reporting agencies
- Minimize, simplify, and streamline data input requirements
- Report only the most essential information

JPAS currently has the capability to report personnel security incidents, using the data input screen shown in Figure 1. Among other things, JPAS is currently being used to track the nature and progress of personnel security investigations for individuals based on SSN and to determine incident criteria based on the adjudicative guidelines. One of the adjudicative criteria—security violations—usually indicates that an information security incident has occurred. Other criteria may sometimes be associated with information security violations.

JPAS does not currently have the capability to report information security incidents. Figure 2a is a mockup of a notional information security incident data input screen for incidents involving possible or probable compromise of classified information. As envisioned here, the screen gathers four types of information (Administrative, Person Reporting Incident, Person of Interest, details of the classified information of concern). The first field input is assigned automatically and the remaining fields are entered as text (12 fields) or check boxes or pull-down menus (13 fields). Figure 2b illustrates the contents of the menus. The screen is designed to be self-evident, easy to navigate, and allow rapid data input. Ideally, a user should be able to fill it out in 1-2 minutes.

Personnel security incidents and information security incidents may be linked if a personnel security incident involving a security violation implies that a reportable information security incident has occurred. The reverse situation is also possible, for example, if an information security incident indicates that the person responsible should be reported in a personnel security incident report. In cases where both types of reports are required, software logic would (1) alert the person completing the input screen, and (2) automatically transfer any redundant information (name, SSN, DOB, citizenship, etc.) to the second report to preclude entering it twice. (An alternative is to combine personnel and information security incident screens so that both types of incidents would be reported in the same place.)

The JPAS information and personnel security incident database would permit a user to run various types of queries within their access scope and authority. Some possible queries are:

- Find all personnel and information security incident records for a given SSN, agency, or agency office
• Determine relative frequency of personnel security incidents based on incident criteria (allegiance to U.S., financial considerations, etc.)
• Determine frequencies of information security incidents by classification levels, information transfer media, or type of information
• Determine frequencies of potential exposures of classified information to unauthorized persons, in the public media, and SCI in the public media
• Determine relative frequencies of disclosures of classified information based on probable causes (negligence, willful misconduct, etc.)

Request for Help

We are asking several DOD agencies and activities to help us judge the feasibility and desirability of implementing the JPAS reporting concept described in this paper. Please review the proposal and share your thoughts with us. Feel free to forward this paper to others in your agency if they have the time and are able to review it. As you conduct your review, here are some issues to consider:

• Feasibility of JPAS incident reporting concept
• Impact on your agency and any related concerns
• Possible use by your agency
• Suggestions and recommendations

By November 11th, please send comments, suggestions, and recommendations to us via email or contact us directly via telephone at:

Eric Lang
• email: eric.lang@osd.pentagon.mil
• phone: 831-657-3025

Henry Simpson
• email: henry.simpson.ctr@osd.pentagon.mil
• phone: 831-657-3056

Fax: 831-645-9060
Personnel Security Incident Report

<table>
<thead>
<tr>
<th>[Person of Interest Name]</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SSN:</td>
<td></td>
</tr>
<tr>
<td>Eligibility:</td>
<td></td>
</tr>
<tr>
<td>Investigation:</td>
<td></td>
</tr>
<tr>
<td>Open Investigation:</td>
<td></td>
</tr>
<tr>
<td>Incident Report:</td>
<td></td>
</tr>
<tr>
<td>Polygraph:</td>
<td></td>
</tr>
<tr>
<td>Foreign Relation:</td>
<td>▼ menu</td>
</tr>
<tr>
<td>Select an Existing Incident:</td>
<td>▼ menu</td>
</tr>
<tr>
<td>Incident Status:</td>
<td>□ Initial □ Follow-up □ Final</td>
</tr>
<tr>
<td>Date of Incident:</td>
<td></td>
</tr>
<tr>
<td>Action:</td>
<td>□ Suspend Access</td>
</tr>
<tr>
<td>Select CAF:</td>
<td>▼ menu</td>
</tr>
</tbody>
</table>

Incident Criteria:
- □ Allegiance to the United States
- □ Foreign Influence
- □ Foreign Preference
- □ Sexual Behavior
- □ Personal Conduct
- □ Financial Considerations
- □ Alcohol Consumption
- □ Drug Involvement
- □ Emotional, Mental and Personality Disorders
- □ Criminal Conduct
- □ Security Violations
- □ Outside Activities
- □ Misuse of Information Techonology Systems

Incident Report

<table>
<thead>
<tr>
<th>Status</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(text field)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 1 JPAS Personnel Security Incident Data Input Screen.
### Information Security Incident Report

#### Administrative Information

<table>
<thead>
<tr>
<th>Report Reference No.:</th>
<th>(computer assigned)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Submission Date:</td>
<td></td>
</tr>
<tr>
<td>Incident Date:</td>
<td></td>
</tr>
<tr>
<td>Incident Investigative Status:</td>
<td>□ ongoing □ closed [date]</td>
</tr>
</tbody>
</table>

#### Person Reporting Incident

| Name and Title: |                     |
| Phone:         |                     |
| Email:         |                     |
| Reporting Agency/Activity: | ▼ menu 1 |
| Organization Code: |                     |

#### Person of Interest

| Name (if known): |                     |
| SSN:            |                     |
| Date of Birth:  |                     |
| Country of Birth: | ▼ menu 2 |
| Citizenship:    | ▼ menu 3 |
| Clearance Level: | ▼ menu 4 |
| Clearance Status: | ▼ menu 5 |

#### Possible or probable compromise of classified information

- Describe information of concern: (text field)
- Classification Level: ▼ menu 6
- Check all of the following that apply:
  - □ Classified information disclosed to unauthorized persons
  - □ Classified information appeared in public media
  - □ US intelligence information disclosed to foreign parties
- Information Transfer Medium: ▼ menu 7
- Type of Information: ▼ menu 8
- Preliminary Inquiry: ▼ menu 9
- Action Taken: □ Damage Assessment □ Additional Investigation
- Likely cause: ▼ menu 10
- Corrective actions taken: (text field)
- Describe any further actions required: (text field)

Figure 2a  Notional Information Security Incident Data Input Screen.
**APPENDIX A**

<table>
<thead>
<tr>
<th>▼ menu 1 - Reporting Agency/Activity</th>
<th>▼ menu 6 - Classification Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Army</td>
<td>none</td>
</tr>
<tr>
<td>CIFA</td>
<td>confidential</td>
</tr>
<tr>
<td>CoCom</td>
<td>secret</td>
</tr>
<tr>
<td>DCMA</td>
<td>top secret</td>
</tr>
<tr>
<td>DFAS</td>
<td>SCI/SAP</td>
</tr>
<tr>
<td>DIA</td>
<td>n/a or unknown</td>
</tr>
<tr>
<td>DISCO</td>
<td></td>
</tr>
<tr>
<td>DLA</td>
<td></td>
</tr>
<tr>
<td>DOHA</td>
<td></td>
</tr>
<tr>
<td>DTRA</td>
<td></td>
</tr>
<tr>
<td>Industry</td>
<td></td>
</tr>
<tr>
<td>Joint Staff</td>
<td></td>
</tr>
<tr>
<td>Navy</td>
<td></td>
</tr>
<tr>
<td>NRO</td>
<td></td>
</tr>
<tr>
<td>NSA</td>
<td></td>
</tr>
<tr>
<td>US AIR FORCE</td>
<td></td>
</tr>
<tr>
<td>US NAVAL</td>
<td></td>
</tr>
<tr>
<td>US MARINE FORCE</td>
<td></td>
</tr>
<tr>
<td>WHS</td>
<td></td>
</tr>
<tr>
<td>other (specify)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>▼ menu 2 - Country of Birth</th>
<th>▼ menu 7 - Information Transfer Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>US or US territory or possession</td>
<td>paper or other hardcopy</td>
</tr>
<tr>
<td>other (specify)</td>
<td>magnetic, optical, or other electromagnetic storage</td>
</tr>
<tr>
<td>n/a or unknown</td>
<td>FAX</td>
</tr>
<tr>
<td></td>
<td>telephone</td>
</tr>
<tr>
<td></td>
<td>email</td>
</tr>
<tr>
<td></td>
<td>internet</td>
</tr>
<tr>
<td></td>
<td>transient electromagnetic (e.g., cell phone, radio transmission)</td>
</tr>
<tr>
<td></td>
<td>transient physical (e.g., briefly exposed classified display screen or board)</td>
</tr>
<tr>
<td></td>
<td>other (specify)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>▼ menu 3 - Citizenship</th>
<th>▼ menu 8 - Type of Information:</th>
</tr>
</thead>
<tbody>
<tr>
<td>US by birth</td>
<td>Foreign government information</td>
</tr>
<tr>
<td>US naturalized</td>
<td>Foreign relations or foreign activities of the United States, including confidential sources</td>
</tr>
<tr>
<td>dual citizenship (specify name of other country)</td>
<td>Military plans, weapons, or operations</td>
</tr>
<tr>
<td>alien</td>
<td>SCI</td>
</tr>
<tr>
<td>n/a or unknown</td>
<td>Scientific, technological, or economic matters relating to national security</td>
</tr>
<tr>
<td></td>
<td>US Government programs for safeguarding nuclear materials or facilities</td>
</tr>
<tr>
<td></td>
<td>US intelligence activities (including special activities), intelligence sources or methods, or cryptology</td>
</tr>
<tr>
<td></td>
<td>US intelligence information</td>
</tr>
<tr>
<td></td>
<td>Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security</td>
</tr>
<tr>
<td></td>
<td>Weapons of mass destruction</td>
</tr>
<tr>
<td></td>
<td>n/a or unknown</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>▼ menu 4 - Clearance Level</th>
<th>▼ menu 9 - Preliminary Inquiry</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>no compromise</td>
</tr>
<tr>
<td>confidential</td>
<td>possible or probable compromise (specify probable recipient)</td>
</tr>
<tr>
<td>secret</td>
<td>certain compromise (specify probable recipient)</td>
</tr>
<tr>
<td>top secret</td>
<td></td>
</tr>
<tr>
<td>n/a or unknown</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>▼ menu 5 - Clearance Status</th>
<th>▼ menu 10 - Probable Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>negligence</td>
</tr>
<tr>
<td>suspended or revoked</td>
<td>willful misconduct</td>
</tr>
<tr>
<td>n/a or unknown</td>
<td>accident or other external cause (describe with mitigating circumstances, if applicable)</td>
</tr>
<tr>
<td></td>
<td>other (describe)</td>
</tr>
</tbody>
</table>

Figure 2b  Pull-down Menus for Information Security Incident Data Input Screen.
APPENDIX B

COMPILATION OF COMMENTS FROM AGENCY VISITS AND FIELD SURVEY
OVERVIEW

This appendix presents agency comments in raw form as we recorded them during discussions and as they were sent to us via email in response to the field survey. The comments are slightly edited for clarity, coded 1-8 based on responding agency, and clustered into subject areas. They do not include technical comments relating to design (e.g., contents of a pull-down menu), although those comments were taken into account in designing the JPAS reporting capability. The comments are summarized in the body of the report under the heading *Agency Reactions to JPAS Security Incident Reporting Concept*. The comments appear below under the same three headings used in the report: *Acceptability of Concept, Agency Concerns, and Issues.*

ACCEPTABILITY OF CONCEPT

- [1] . . . we think this would be beneficial to [agency name] and to contractors. We agree with the benefits outlined in the paper.
- [2] will accept JPAS reporting concept
- [3] [agency name] would accept JPAS reporting concept
- [3] we have some violations again and again
- [3] we handle incidents locally; handling incidents locally does not tell you if you have a problem
- [3] [agency name] now tracks commander’s evaluations—may not reveal all problems
- [3] JPAS reporting could be a good function for OSD to tell what is wrong
- [3] we cannot currently get stats on violations; to get them we would have to issue a very labor intensive data call—this proposed system would permit it, very useful
- [3] [do] not support ISOO getting security violations. USDI and ISOO can get enough information from JPAS that is not tied to an individual. The MILDEPS should be given the security violations and then an annual report could be sent to DSSA, through USDI, with the bottom line of the security violations. This way DSSA can create courses that are directly related to the security violations that occur according to the annual reports. ISOO should be for oversight and not reviewing security violations.
- [4] I’ve read your paper with great interest. Since it addresses a logical and what I would hope would be a relatively non-controversial initiative, I don’t have much to add beyond a few simple remarks.
- [4] Should the software be appropriately configured and the JPAS platform support its functionality reliably it ought be technically simple enough.
• [4] **Impact, Related Concerns.** I wouldn't expect adverse impact; the workload is not high as it is. Favorable program impact would have to be adjudged in the offing.

• [4] **Possible Use.** Centralizes infosec incident information electronically; may support information security management program via relational database queries targeting departmental, organizational, individual trending; relates to continuing evaluation assessments.

• [4] . . . the information security incident screen is worth pursuing. I believe feasibility is best seen as proven in judgment of the quality of local execution after the screen and attendant policy are established. It ought be easy enough; it transfers, or redounds, info otherwise documented in paper to the electronic document, where the information can also be used for corollary departmental purposes.

• [4] **Feasibility:** . . .Where feasibility becomes rather more subjective is in policy and compliance. It would difficult for me to conceive of policy that caused a noteworthy increase in reportage of personnel security incidents. Most of what the proposal centers upon has to do with the traditional notification of security headquarters elements, by organizations within their jurisdictions, of the occurrence of a behavior, syndrome, arrest, etc., etc. which is of such a troubling nature that the organization’s laymen believe it best to elevate it as a potential national security protection-related issue. This seems to occur at a low frequency, given the immense number of individuals and organizations embraced by the personnel security program and the great difficulty the Department has historically faced in clarification for supervisors as to what a relevant continuing evaluation issue actually is at the sub-trauma level. The emergence of a JPAS alteration will not change that in my view.

• [5] **Feasibility of JPAS incident reporting concept - Support the JPAS reporting concept and standardizing incident reporting.** The way this is written if there was no possibility of compromise a information security incident would not be reported. Therefore, a person could have several incidents and as long as there was no possibility of compromise they would not have to be reported.

• [5] **Impact on your agency and any related concerns - Reporting responsibilities should not vary by Agency (as stated in attached) and it's extremely important to adhere to those reporting requirements.** Often security incidents that are not considered security violations are not reported to Personnel Security. Therefore not providing any type of tracking mechanism for repeated incidents that may have occurred on an individual.

• [5] **Possible use by your agency - Will be used for reporting requirements and reports of incidents.**

• [5] Even when inquiry/investigation determine there is no compromise, if potential for compromise is due to failure of a person or persons to comply with established security practices/procedures, this would then fall under the reportable item for Personnel Security (Adjudicative Guidance: Noncompliance
with security regulations raises doubt about an individual’s trustworthiness, willingness, and ability to safeguard classified information).

- [5] If all DOD consistently reports by JPAS then perhaps weaknesses and/or vulnerability of an individual or individual’s who may have several "security incidents," will be noticed and considered or at least flagged for further investigation, especially if other security incidents/concerns have been reported such as foreign contact/association and financial.

- [6] . . . I sent your concept paper out to several of my fellow security co-workers and have attached their comments. Overall, we see it as feasible and that it would have no great impact on our Agency other then granting JPAS access to our Information Security Staff for reporting the incidents. We would definitely use it as we now do to report access suspensions. Please let me know if you have any questions.

- [6] I think it would be very beneficial to do this. It should be integrated into the adjudicative process; i.e., habitual offenders should not hold clearances.

- [6] I see this as a good thing; it tightens the system up in that a quick review will allow an analysis of training needs, problem areas and potential problem employees. Anything that gives us more insight into security risks will allow us to plug more of the holes. I don’t know enough about the current automated systems to be able to say whether this will simplify reporting or add an additional burden but the premise is good and gives hope for the future.

- [6] This sounds like a good idea. It will save the DOD agencies from having to report to DUSD (Cl&S) directly. They can pull their own reports from JPAS.

- [7] concept is good, this could be useful

- [7] would like to get a request from USDI framing a vision

- [8] This would be a great tool to collect and store security incidents and violations. DOD needs a central database where information like this can reside.

- [8] The impact to our agency would be positive. [Agency] has approximately 50 JPAS users who I believe would find value in the system and utilize it. Here again, my concern would be user roles and rights.

- [8] The feasibility of JPAS incident reporting concept is logical. This is the perfect place for an incident reporting system. Adjudicators at the CAF will have access to it to as well as specialists in the field.

**AGENCY CONCERNS**

**Additional Reporting Burden**

- [2] do not increase workload; sounds like using JPAS will increase workload

- [2] do not want to duplicate reporting in JPAS and local system

- [2] current problem with JPAS—need help in JPAS to support end users
APPENDIX B

- [2] intelligence reporting
- up through DNI
- 6/8 tells what DNI regards as “significant incidents”
- 5-6 different categories
- [2] NRO has security incident reporting database—deals with infosec and personnel security
- [7] administrative burden - possible administrative burden for 4000+ commands

**Usurpation of Agency Prerogatives**

- [2] JPAS reporting model
- permits CAFs to get involved in local decision-making
- previously was done in units
- better guidance needed re how to use info in JPAS
- problem—how to report data and not take action on it (discussion—perhaps establish rules that define what triggers action)
- [2] We have additional concerns regarding the privacy of information about individuals involved in security violations. There can be considerable differences between the what, who, how, when and where reported in initial reports and what is reported in subsequent follow-up reports and final reports. In short, information taken out of proper context could be unnecessarily and inappropriately prejudicial to individuals whose names are included in reports. Ensuring this does not happen or fixing it when it does could itself become an administrative burden on SSOs.
- [3] we do not want an adversarial system. we have enough trouble to get people to follow rules
- [7] usurping authority
- admin incidents—COs should be able to handle
- are we taking away some of the authority of COs and security managers?
- [7] protecting individuals
- possible problems for individuals caused by associating violations in JPAS with name
- concern about possible misuse of information

**Miscellaneous Concerns**

- [3] often don’t have time to collect all information
- [3] concern that JPAS would not get the report
• [3] investigators often lack needed skills, may lack training, don’t know what to look for
• [7] data quality
• JPAS already is not being used properly—still has a potential for flaws
• need to consider entire environment, not just office; data might be flawed by constraints
• [8] One of my concerns is will all of the CAFs utilize this system. Currently all of the CAFs do not fully utilize JPAS and all of the functionality within the system. It makes no sense to have a DOD-wide system that is not utilized by all.
• [8] My concern is if access suspension will be linked to this system; and, if so, who will be able to suspend access and will this information flow to JPAS. While I think it’s a good idea to have a system that the adjudicators can use to see information they may or may not become aware of, we don’t want to overload them with an additional workload. Unnecessary access suspensions could generate more work for the adjudicators if accesses are suspended inappropriately.

ISSUES

Clarify Terminology
• [2] “violation, incident” terminology needs careful definition
• [3] In reviewing the Concept Paper, there needs to be guidelines on what security violations will be included into JPAS. Currently, the term incident is being used as an overall term and violations and practices dangerous to security (PDS) are two types of incidents.
• [3] terminology—usually use “incident” in relation to information security and “violation” for personnel security
• [3] merge security violations and incident reporting
• [6] The concept paper’s title contains the word “violation.” The first and second paragraphs do not refer to “violations” but to “incidents.” Most subject matter experts treat incidents as events worthy of further investigation and/or adjudication. Violations have been fully investigated and adjudicated as significant. What will the proposed system memorialize: incidents or violations?
• [6] Recommendation: Include widely recognized definitions for terms in future drafts of the concept paper and use terms consistently in the drafts.

Provide User Guidance
• [2] non-compromise incidents do not have to be reported in JPAS
• [3] . . . specific guidance will need to be included as to what is a security incident, security violation, and whether a PDS will also be included. There really is not a definition on security incident, other than a compromise of
information. What will constitute an incident/violation having to be input into JPAS? If there is no compromise, but there is a security violation (e.g., container not locked in a SCIF - no compromise but violation) is the information to be added into JPAS? Bottom line, there needs to be specific guidance as to what will be added and what will not be added to JPAS. Remember, this will be a permanent record that will follow an individual wherever he/she goes.

- [3] currently most security viols are not reported as incidents but should be
- [3] we need to define what justifies an incident report
- [3] I understand that DUSD(CI&S) oversees both information and personnel security programs, but I think you either need to more clearly identify which security incidents you are talking about or make two separate concept papers - Security Violations and Personnel Security Incidents. Blanket statements are made about security incident reports and if this turns into a policy paper, more specifics need to be provided which are in discussion.
- [6] Need to limit who can enter reports
- [6] Also, need rules on when reports are entered. If a report is entered prematurely, the “person of interest” may be inappropriately branded with derogatory information before his/her guilt has been determined.
- [6] Recommendation: DUSD (CI&S) develop a classification guide prior to system design for its mission of consolidated security incident/violation reporting. System users would then be able to enter information with assurance that they are not committing a security violation by unknowingly entering classified information into an unclassified data system.
- [6] Recommendation: DUSD (CI&S) develop a classification guide prior to system design for its mission of consolidated security incident/violation reporting. The classification guides for Critical Infrastructure Protection and Information Operations address similar situations now.
- [7] written guidance needed
- what will be guidelines?
- do not know of a requirement to provide information to DOD
- DOD has to provide adequate guidance for electronic (IT) environment
- [7] reporting thresholds
- hesitant to deal with every safe, visitor, etc.
- espionage—no need to track
- deliberate and willful release is rare; inadvertent is common
- electronic information is fairly scary; lots of incidents because they are inadvertent; classified information is “dumbed down” for transmission
- incidents vary in importance--important: compromise of information, public release; criminal loss
• 2 types of incidents: threshold (human error), violation

• [7] DOD has failed to provide adequate guidance for dealing with routine issues; community wants 2-R and 1-R

**Report and Database Classification Level**

• [3] The screen titled, "Information Security Incident Report," there is information that should already be in JPAS on the individual, such as the person's country of birth (menu 2), citizenship (menu 3) and the person's clearance level (menu 4). This is redundant information. Also, there is too much information/details on the information security incident to be placed on an unclassified system. If all menus are completed on the unclassified system, and it ever gets hacked into, I could find out that the Army had a S/SCI document, with the description of the information, placed on the SIPRNET. [This agency] has no problem with including menus 1, 5, 6, 9, and 10, but we need to be very careful with menus 7 and 8. In the SCI arena, if there has been a compromise of classified information in the media, DIA would like the report to be at least CONFIDENTIAL. This would eliminate the ability to add the information into JPAS.

• [6] The memorializing of security incident/violation information may be "classifiable" depending on the context of the event. The concept paper proposes the system would be used for data entry of unclassified information. However, it does not prescribe the use of an existing classification guide to assist the user in determining classification of information slated to be entered.

• [6] The concept paper specifies the entry of only unclassified information. Individual records in the data repository will therefore be unclassified. However, the data repository will probably be classifiable because it will be the aggregate of the Department’s documented incidents/violations. Also, the use of the data mining tools by Department or component researchers will likely produce reports containing classified aggregates that can not be properly labeled for display in a workstation in an unclassified environment without the logic of a classification guide.

**Inclusion of SCI-Related Information**

• [2] Although we are not opposed to the concept, we cannot concur with the process of reporting security incidents involving Sensitive Compartmented Information (SCI) via JPAS until other matters bearing on SCI reporting procedures are addressed. However, because of the authority and responsibility chain for SCI and the sensitivity of the information involved, it is our recommendation that security incidents involving SCI, which is under the cognizance of the Director of National Intelligence, be excluded from this process. Duel reporting, via Special Security Office (SSO) System channels to meet IC reporting requirements and via JPAS to meet DOD reporting requirements would place an unacceptable workload on our SSOs. The following is provided in explanation/support of this position.

reporting involving intelligence information. DOD 5105.21-M-1, Sensitive
Compartmented Information Administrative Security Manual (referred to as the
M-1) implements DCID 6/8 for the DOD. DOD 5200.1-R appropriately defers
to the M-1 for reporting security incidents involving SCI. Any change in SCI
incident reporting procedures must be addressed in the M-1, which is currently
under revision.

- [2] 2. The process for handling collateral security
incidents/violations/compromises differs significantly from that of the
Intelligence Community. Within the Air Force, most collateral incidents are
essentially handled at base level and reported only as statistics to higher
headquarters. Security violations involving SCI, on the other hand, are
all reported to higher headquarters, DIA, and in certain cases to the DNI.
Additionally, reports are often classified themselves, to protect the information
involved from whatever perceived vulnerability may exist at the time the SSO
reports an incident, or they contain classified information actually involved in
the incident.

- [2] 3. The M-1 requires that security violations involving SCI be reported to
DIA/DAC-3D within 72 hours. The M-1 and the Joint DOD IIS/Cryptologic SCI
Information Systems Security Standard (JDCSISSS) both require all security
violations occurring on information systems that process SCI be reported
through command SCI channels to the appropriate SOIC with information
copies to DIA/DAC-3D/SYS-4. NSA requires such reports be classified a
minimum of Confidential. In DCID 6/8, the DNI has charged SOICs to promptly
notify the DNI of any significant security violation, unauthorized disclosure, or
other compromise. All these reporting requirements must be addressed to
eliminate duplicative and unnecessary reporting channels.

- [2] 4. The Intelligence Community also has a database for recording security
incidents involving SCI. The database is currently used for incidents occurring
on information systems, but it is being developed for use for all incidents
involving intelligence information under the cognizance of the DNI. We highly
recommend that DOD processes for security violation reporting be coordinated
with the DNI to insure Special Security Offices are not burdened with duel
reporting channels.

**Reporting of Personnel Security Incidents in JPAS**

- [4] Most personnel security-related incidents are dealt with via PSI and
adjudication, for which JPAS has, or is developing, tools sufficient to DUSD(I)
reportage . . . Consequently, I see no need to go beyond information security]
incident reporting . . .