PERSEREC

Technical Report 13-06
November 2013

The Evolution of the Automated Continuous Evaluation System (ACES) for Personnel Security

Katherine L. Herbig
Northrop Grumman Technical Services

Ray A. Zimmerman
Northrop Grumman Technical Services

Callie J. Chandler
Defense Personnel and Security Research Center
Defense Manpower Data Center

Approved for Public Distribution: Distribution Unlimited
Defense Personnel and Security Research Center
Defense Manpower Data Center

Technical Report 13-06 **November 2013**

The Evolution of the Automated Continuous Evaluation System (ACES) for Personnel Security

Katherine L. Herbig—*Northrop Grumman Technical Services*
Ray A. Zimmerman—*Northrop Grumman Technical Services*
Callie J. Chandler—*Defense Personnel and Security Research Center/DMDC*

Released by – Eric L. Lang

BACKGROUND

The Defense Personnel and Security Research Center (PERSEREC) developed the Automated Continuous Evaluation System (ACES) over a period of 20 years. Initially, ACES was intended to check electronic records for continuous evaluation (CE) in the Department of Defense (DoD) during Periodic Reinvestigations (PRs) for security clearances. Since 2008, the Joint Reform Effort (JRE) of the federal government has identified ACES as a capability to include in the revised federal security clearance process, and various pilot projects have demonstrated ACES' capabilities for different federal agencies and with different types of investigations.

HIGHLIGHTS

ACES is an automated computer system that collects data from over 40 government and commercial databases. It uses an applicant's personally identifiable information (PII) or the Standard Form 86 (SF-86) to check these data sources, verify what has been submitted, and collect more information. It applies business rules to the data, produces a report that flags issues of potential security concern, and electronically transmits the report to the approved recipient—typically an adjudication facility.

ACES is scalable to handle five million requests per year in a robust, flexible, and expandable automated system. Pilot projects have demonstrated that ACES will streamline the expensive security clearance and suitability vetting process and greatly reduce its cost. ACES can be used between background investigations, to replace elements of initial investigations or reinvestigations, to prescreen military recruits, and in counterintelligence investigations. ACES can harness the power of automation to reduce costs, improve timeliness, and expand the range of information available to those who seek reliable, loyal, and trustworthy personnel.

Defense Personnel and Security Research Center
Defense Manpower Data Center
400 Gigling Rd.
Seaside, CA 93955

REPORT DOCUMENTATION PAGE

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

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE: 20131112	2. REPORT TYPE Technical Report 13-06	3. DATES COVERED Oct. 1989 – Nov. 2012
4. The Evolution of the Automated Continuous Evaluation System (ACES) for Personnel Security	5a. CONTRACT NUMBER:	
	5b. GRANT NUMBER:	
	5c. PROGRAM ELEMENT NUMBER:	
6. AUTHOR(S): Katherine L. Herbig, Ray A. Zimmerman, Callie J. Chandler	5d. PROJECT NUMBER:	
	5e. TASK NUMBER:	
	5f. WORK UNIT NUMBER:	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Defense Personnel and Security Research Center 400 Gigling Rd. Seaside, CA 93940	8. PERFORMING ORGANIZATION REPORT NUMBER PERSEREC: Technical Report 13-06	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITOR'S ACRONYM(S)	
	11. SPONSORING/MONITOR'S REPORT NUMBER(S):	

12. DISTRIBUTION/AVAILABILITY STATEMENT: (A) Distribution Unlimited

13. SUPPLEMENTARY NOTES:

ABSTRACT: The Automated Continuous Evaluation System (ACES) was developed by the Defense Personnel and Security Research Center (PERSEREC) through iterations of research and application of research findings to improve versions of ACES. ACES is an automated computer system that collects data from over 40 government and commercial databases. It uses an applicant's personally identifiable information (PII) or the Standard Form 86 (SF-86) to check these data sources, verify what has been submitted, and collect more information. It applies business rules to the data, produces a report that flags issues of potential security concern, and electronically transmits the report to the approved recipient—typically an adjudication facility. Since 2008, the Joint Reform Effort (JRE) of the federal government has identified ACES as a capability for inclusion in the revised federal security clearance process, and various pilot projects have been performed demonstrating ACES' capabilities for different federal agencies and with different types of investigations. Pilot projects have demonstrated that ACES will streamline the expensive security clearance and suitability vetting process and greatly reduce its cost. ACES can be used between background investigations to replace elements of initial investigations or reinvestigations, to prescreen military recruits, and in counterintelligence investigations. ACES can harness the power of automation to reduce costs, improve timeliness, and expand the range of information available to those who seek reliable, loyal, and trustworthy personnel.

14. SUBJECT TERMS: Automated Continuous Evaluation System (ACES), Security Clearance, Personnel Security, Automation, Electronic Records, Adjudication, Automated Records Checks (ARC), Joint Reform Effort (JRE)

15. SECURITY CLASSIFICATION OF: UNCLASSIFIED			16. LIMITATION OF ABSTRACT:	17. NUMBER OF PAGES: 61	19a. NAME OF RESPONSIBLE PERSON: Eric L. Lang, Director
a. REPORT: UNCLASSIFIED	b. ABSTRACT: UNCLASSIFIED	c. THIS PAGE: UNCLASSIFIED			19b. TELEPHONE NUMBER (Include area code): 831-583-2400

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

PREFACE

The Department of Defense (DoD) currently grants more than two million employees and contractors eligibility for access to classified or sensitive information, or for positions of trust, which include work with children, physical access to sensitive facilities, and logical access to DoD information technology systems. Each security clearance or access requires a background investigation, an adjudication decision based on a review of the investigation, and related procedures such as recording and maintaining the information that has been collected to ensure the clearance or access holder's privacy and the availability of the information for future actions, and providing fair due process and appeals procedures. Standards for granting such eligibilities, and the basic steps in the process, date from early in the Eisenhower administration, although since then they have been repeatedly revised and updated. Nevertheless, DoD spends millions of dollars annually on these security clearances and accesses, seeking to ensure that only loyal, trustworthy, and reliable persons are granted eligibility.

The Automated Continuous Evaluation System (ACES) offers DoD a cost-effective, automated way to check electronic records on applicants for a security clearance or position of trust early in a background investigation. Pilot projects have repeatedly demonstrated that ACES locates issues of security concern about applicants as well as and often better than human investigation, does it faster, and does it at a fraction of the cost. Since the federal government is moving to a consistent personnel security process for clearances across agencies, ACES could become part of the Automated Records Check (ARC) step in the new government-wide system once it is adopted. The ACES system, originally developed for DoD, also could then be scaled up to become available to all government agencies that grant eligibility for security clearances or positions of trust.

Eric L. Lang
Director, PERSEREC

EXECUTIVE SUMMARY

This report explains how the Automated Continuous Evaluation System (ACES) was created, how it currently works, and how it could be used in the future. The Defense Personnel and Security Research Center (PERSEREC) developed ACES for the Department of Defense (DoD) as an automated system to support continuous evaluation (CE) of personnel with security clearances by checking electronic databases in-between the 5-year or 10-year intervals for periodic reinvestigations. Currently, PERSEREC is demonstrating through a series of pilot studies how ACES would contribute to additional types of background investigations by federal agencies across the government.

ACES is an automated computer system that collects data from more than 40 government and commercial electronic records. It uses an applicant's personally identifiable information (PII) obtained from the federal security questionnaire, the Standard Form 86 (SF-86) to check these data sources, verify the information that has been submitted, and leverage the information gathered to collect additional subject information. It applies business rules to analyze the data returned, produces a report that flags issues of potential security concern, and electronically transmits the report to the approved recipient—typically an adjudication facility.

PERSEREC's early work during the 1990s on what would become ACES dealt with automating credit reports, tapping electronic databases that were just becoming available, and improving documentation of security clearance applicants' past financial and criminal behavior. In 1999, DoD[1] requested that PERSEREC plan a prototype of an automated system. The request directed that the system should be capable of (1) pulling information on applicants from each specific database in the study; (2) assessing whether the derogatory information returned by the searches exceeded established thresholds; (3) assessing when information returned should trigger an aperiodic reinvestigation; and (4) electronically forwarding results from the searches for dissemination to investigators and adjudicators.

Based on that initial prototype, ACES development has been incremental, building systematically on the results and revisions from each previous pilot study; it has been practical, seeking and incorporating feedback from potential users at each step in order to maximize the program's usefulness; and it has been pragmatic, responding to new customers as their interest and funding allowed. ACES constantly evolved, but each ACES check focuses on concerns in one or more of the 13 Uniform Adjudicative Guidelines, the latest version of which was adopted in 2005.

There have been two versions of ACES. Version One operated between 2004 and 2009. In Version One, some interactions were computer-to-computer and fully

[1] In 1999, the relevant DoD entity was the Office of the Assistant Secretary of Defense (Command, Control, Communication, & Intelligence [C3I]).

automated, others were indirect, in that a request for data would be sent to data providers who ran the check themselves and sent the resulting data back to an ACES operator. The third and most common type of interaction was computer-to-computer with some manual intervention required by the ACES Operator to load data or start software. The system capabilities of the various data providers and the nature of their electronic files dictated this variety of approaches. Version One could initiate about 5,000 checks per week. Since some indirect checks relied on the mail, it could take several weeks to complete one batch of ACES checks.

Starting in 2004, Congressional action, and criticism of DoD's personnel security system by the Government Accountability Office (GAO), led to the formation of the Joint Reform Effort (JRE) to coordinate serious government-wide reform. ACES offered a successful and functioning automated system for checking security-related electronic records, and it was referenced as a key element in the reformed vision for the federal personnel security system. PERSEREC began to plan for a broader application of ACES beyond DoD.

A reformed system, as proposed by the JRE in 2008, would collect and validate more information about a security clearance applicant early in the process through an expanded electronic application and Automated Records Checks (ARC) of electronic databases using an automated system such as ACES. Next, automated business rules would scan the information collected for issues, flag any issues of security concern, and electronically adjudicate (eAdjudicate) cases to make a risk assessment decision. Clean cases—those without flagged issues—would need no further human handling. Only then, if necessary, an investigator would interview the applicant in person about the issues. In this way ACES efficiently sorts cases requiring human intervention from those that do not. These steps built on PERSEREC's earlier research on productivity of sources and phasing of the investigation.

Thus, starting in 2008, the direction of ACES research and development shifted to reflect the goals of the JRE and the emerging national program. ACES researchers undertook a series of pilot studies for various federal agencies starting with the first version of ACES and continuing on with the second version to demonstrate ACES' capabilities in various types of investigations, in various experimental conditions, while comparing ACES' proficiency against the ARC capabilities of other agencies and traditional investigations by various providers.

The JRE's new vision for the ARC component prompted the need to revise and expand the ACES system. ACES would no longer be limited to the role of CE, but was being integrated into the initial background investigation, and it would reach beyond DoD personnel and contractors to a wider population including other departments of the federal government. Its automated checks would apply not only to individuals with Top Secret (TS) and Sensitive Compartmented Information (SCI) access, but also to those seeking a Secret (S) clearance and positions of trust that do not require a security clearance but do require a background check.

Policymakers also requested new features be added to the ACES system, such as a la carte checks and a web service interface. These changes in how ACES would be used meant the system would be dealing with a greatly expanded scope, and the volume of checks would increase greatly. To accommodate the JRE's vision for an integrated security clearance program across the federal government, it was necessary to update and expand ACES in Version Two.

Changes in organizational context within DoD were a second important influence shaping ACES. Since DoD had supported and sponsored ACES from its inception, organizational changes in DoD affected ACES' development. Two changes in DoD especially influenced ACES: (1) the transfer of DoD's background investigations to the Office of Personnel Management (OPM) in 2005, and (2) the creation of the Defense Information System for Security (DISS) in 2009. Both of these brought additional players and competing agency interests into ACES development.

Version Two will be scalable to process up to five million cases per year. ACES would need to take advantage of newer technologies that had developed or matured since the development of the ACES Version One, including:

- Infrastructure independence: it will function on different hardware and software platforms to mitigate the negative consequences of vendor lock-in.
- Modularity: each major function or external interface of the system will be designed as a separate software component separated by logical boundaries, with a clearly defined interface for communicating with the component.
- Loose coupling: major software components would be replaceable without affecting other components of the system.
- Scalability: the hardware and software architectures will accommodate an increased volume of ACES checks.
- Extensibility: it will incorporate new types of checks in the future.
- Comprehensiveness: it will provide support for lifecycle management processes.
- Flexibility: it will meet the changing needs of users.

More powerful hardware and software changes improved the speed of external interfaces to data providers, allowed faster processing of records, and increased the number of cases the system could store. A new Web Services Interface was developed that worked via a computer-to-computer interface to allow user agencies to directly request checks and download reports across the Internet.

The ACES program using Version Two undertook three pilot studies for various federal agencies in 2012, and continues with several others in 2013. Repeated demonstrations in various agencies and with various types of investigations have proven that ACES will streamline the expensive security clearance and suitability vetting process and greatly reduce its cost. ACES electronic database checks can be used between an initial background investigation and a periodic reinvestigation, during the career of a clearance-holder between regular reinvestigations, as a

replacement for elements of the initial or the reinvestigation, as a tool for prescreening military recruits, and as a tool for counterintelligence (CI) investigations. From its beginnings, the promise of ACES as an automated personnel security solution has been its ability to harness the power of automation to reduce costs, improve timeliness, and expand the range of information available to those who seek reliable, loyal, and trustworthy personnel.

TABLE OF CONTENTS

LIST OF FIGURES

INTRODUCTION

This report provides an overview of the development of the Automated Continuous Evaluation System (ACES). Later sections discuss its current capabilities and its potential for expansion or new applications. ACES grew out of several projects undertaken at the Defense Personnel and Security Research Center (PERSEREC) to support personnel security adjudication at Department of Defense (DoD) facilities. These initial projects were aimed at helping adjudicators make better use of information from an electronic database, e.g., by producing more readable credit reports. Over a period of years, the system grew into one that can collect a broad array of background information from multiple electronic databases, combine it into an adjudicator-friendly report, and flag information of potential concern.

At first, the concept of ACES focused on developing a system to supplement the periodic reinvestigation process for personnel with eligibility for access to classified information. Individuals with Secret (S) eligibility must be reinvestigated at 10-year intervals, and those with Top Secret (TS) eligibility must be reinvestigated at 5-year intervals. Typically, during those intervals, no information would be collected about the person. For years, personnel security officials would have little insight into changes or evolving problems in a cleared individual's life that could indicate security concerns. ACES was intended to open a window for adjudicators into the intervals between periodic reinvestigations. It could supplement those investigations with regular but aperiodic, and therefore unpredictable, checks of electronic databases.

Recently, officials working to reform the federal personnel security system have recognized the wider usefulness of ACES, and PERSEREC is exploring how to apply it in additional types of background investigations by agencies across the federal government. Research has demonstrated that ACES can augment and, in some cases, replace traditional background investigations, saving time and money.

In its current form, ACES is an automated computer system that collects data from more than 40 government and commercial electronic records. When an agency requests an ACES check, ACES uses an applicant's personally identifiable information (PII), if that is available, or it uses the responses to the federal security application, Standard Form 86 (SF-86), the *Questionnaire for National Security Positions*, to initiate the check. The system runs checks against the data sources to verify the information an applicant has submitted, or to collect more information about the person. There is a nominal fee for each data check. ACES analyzes the data that has been returned using business rules developed by adjudicators, security policy officials, and CI experts. It then produces a report that flags issues of potential security concern, and electronically transmits the report to the approved recipient.

Development of ACES has proceeded through a series of pilot studies sponsored by various government agencies; each pilot study has tested applications of ACES in

different configurations. For example, configurations may be set to define how subjects will be selected for ACES checks, which data sources will be checked, how business rules that analyze the data are calibrated, and which checks are to be run. ACES is not yet in production as a federal personnel security capability, but the system is under consideration by numerous agencies and is being pilot tested in several new applications, including military accessions and Department of State (DoS) investigations.

THE EARLY YEARS OF ACES DEVELOPMENT

ACES grew out of a series of projects undertaken during PERSEREC's first decade, starting in the late 1980s and accelerating through the 1990s. In these projects, as in all PERSEREC's work, researchers sought to make the personnel security system more efficient, fair, and effective; the projects that led to ACES were focused on those goals. Projects that became building blocks for ACES dealt with automating credit reports, tapping electronic databases, and improving documentation of security clearance applicants' past financial and criminal behavior.

FIRST STEPS: AUTOMATING CREDIT REPORTS AND FINANCIAL DATA

In 1989, PERSEREC designated "Financial and Credit" as one of its program areas,[2] and began work to improve the information collected on finances and credit in background investigations conducted by the Defense Investigative Service (DIS).[3] At that time, DIS performed most of the background investigations for DoD personnel. One project worked with adjudicators, investigators, and case controllers to develop a user-friendly report format that was written in plain English, not in proprietary codes. It also pulled all the needed information together in one document, highlighted relevant information in the order requested, and provided a summary (Timm, 1997). Another project eliminated costly redundancies in the information DIS gathered from the three national credit bureaus by improving the automated routines DIS used to interact with the credit bureaus. PERSEREC demonstrated that requesting no more than one report per applicant from each credit bureau, rather than a separate report from each bureau for each address the subject reported living at during the scope of the investigation produced identical data, eliminated duplication, and eliminated the need to run one-third of the credit reports typically requested by DIS. Each of the three credit bureau inquiry formats allowed the entry of multiple addresses on a single report request. The contractor acquiring credit reports for DIS implemented the multiple address inquiry change at once, which immediately reduced what it charged for credit checks. Estimates at the time projected savings to the DIS credit acquisition budget from this change alone of 14.6% (Timm, 1990; Timm, 1997).

In the early 1990s, when PERSEREC began to study it, the process for gathering credit information on an applicant for a security clearance was laborious: reports from credit bureaus were printed out; clerks manually reviewed the paper files from multiple bureaus and collated the unique derogatory data received across bureaus; other clerks microfilmed the records of cases with security issues for storage and shredded the non-issue reports; credit bureau reports arrived in technical formats

[2] This reflected the fact that over the previous decade espionage by American citizens most often had been motivated by financial need or by greed for more money (Herbig & Wiskoff, 2002; Herbig, 2008).

[3] In 1997, DIS's name was changed to the Defense Security Service (DSS).

that were proprietary to each bureau, requiring case controllers to translate the results using differing credit bureau manuals. A case controller manually applied DIS financial business rules to determine whether a case needed more work; when manual calculations found one or more problems that violated the business rules, it was deemed an issue case and sent for additional investigation and data collection.

PERSEREC developed a prototype data collection and analysis system for credit reports that could successfully draw in data from all three of the national credit bureaus, eliminate duplicate information from them, and identify the cases of concern based on the same DIS financial business rules case controllers were already using. Responding to that success, DIS provided PERSEREC $10,000 to contract with an independent developer of credit report systems to build something similar, an automated credit report acquisition and analysis system. In 1994, DIS adopted PERSEREC's Automated Credit System.

The system improved the request process, produced more information from the three credit bureaus, and paid for itself in the first 3 weeks of operation. The computer program added the applicant's delinquent accounts, if any, and applied decision logic tables supplied by DIS to determine automatically whether the case had security issues. Since most applicants do not have security issues, the computer identified those and declared them non-issue cases without further human contact. Whole forests were saved by printing only the minority of cases with security issues for adjudicators to consider, along with a one-page credit summary on the nonissue cases that displayed the data adjudicators felt would be most valuable in making a decision. An electronic copy of all credit reports (from non-issue as well as issue cases) was saved for future reference and comparison. Security personnel could easily read the credit reports in their new, readable format that saved them time, and if duplicate credit information on an applicant was received from more than one bureau, the system detected the duplication and only printed one trade line with that information. By demonstrating how automation could reduce manual intervention, increase efficiency, save money, and improve the information available to adjudicators, PERSEREC captured the backing of DoD officials at the Office of the Secretary of Defense, Command, Control, Communications and Intelligence who supported using automation to make further reforms to the personnel security system (H. W. Timm, personal communication, April 19, 2012; Timm, 1997).

CHECKING LARGE CURRENCY TRANSACTIONS

Another ACES building block was the incorporation of the Department of the Treasury's (DoT) database of transactions that come under U.S. Code Title 31, the Bank Secrecy Act. This legislation requires that the government track large currency transactions, defined as those of more than $10,000 in cash, which move into or out of financial institutions and casinos. Checking DoT's Financial Crimes

Enforcement Network (FinCEN) for large transactions helps to identify and prosecute money laundering, tax evasion, and various forms of fraud (Internal Revenue Service [IRS], *Manual*, n.d.). Since spies usually receive payment in cash, these transactions can also indicate movement of money from crimes such as espionage. PERSEREC brokered a memorandum of understanding in 1995 between DoT and DoD to share data, and developed an automated system for identifying clearance applicants who had made large currency transactions that should be evaluated to see if the person had accurately filed Title 31 disclosure forms.[4] The automated system submitted these names to FinCEN, acquired the relevant data electronically, and then returned the data in a format that DoD adjudicators had requested. DIS incorporated this system on large currency transaction checks into its background investigations in 1996 (Timm, 1997).

AN EARLY REFERENCE COLLECTION ON PERSONNEL SECURITY DATABASES

PERSEREC also compiled a reference collection of commercially available computerized information sources relevant for personnel security investigators and adjudicators. Published in 1991, the report described and evaluated each source for its usefulness in locating individuals or providing data on their issues with financial, credit, real estate, bankruptcy, income, or spending habits ("Commercial databases," 1991). Armed with this familiarity with electronic databases and financial and credit data, researchers consulted DIS investigators and adjudicators at the various DoD adjudication facilities seeking to understand the particular data needs and problems with access to data that they faced. Knowing the databases that were being made available and the data needs and problems of potential DoD users of that data, PERSEREC realized that a structured automated system to search and organize the electronic data that was becoming more available would streamline the personnel security process. Building on the initial work with DIS on credit report requests, the next project that laid the foundation for ACES focused on automating the acquisition and screening of credit reports during background investigations (H.W. Timm, personal communication, April 19, 2012).

FINANCIAL MOTIVES FOR ESPIONAGE

What most of the early projects that advanced ACES development had in common was money. They focused on automated ways to check on clearance applicants' financial behaviors using databases of credit and financial records. In 1994, the arrest and conviction for espionage of Aldrich Ames, a Central Intelligence Agency (CIA) officer working in Soviet CI, had underlined the importance of money as a motive for espionage. Ames' espionage financed his unexplained affluence that

[4] Research supporting development of this automated system was conducted jointly by PERSEREC, FinCEN, the U.S. Customs Service, and the Defense Manpower Data Center (DMDC) (Timm, 1997).

continued unexamined by his agency for years, and since he was paid for his information in cash, he had filed three large currency transactions (U.S. Senate Select Committee on Intelligence, 1994; "New DoD Personnel Security Program," 1995). The Ames case prompted a federal requirement that government employees who, like Ames, can have access to especially sensitive information, must file annual financial disclosure statements so that better oversight can be exercised to deter and detect crimes for profit[5] (Executive Order [E.O.] 12968, 1995). In response, PERSEREC helped develop a financial disclosure statement form in 1996 and began work on an automated system for analyzing the information reported on the disclosure forms for unexplained affluence or fraud. The CIA, smarting from criticism over Ames' betrayal, implemented the form a year later and worked with other intelligence community (IC) agencies and with PERSEREC on automating the analysis of financial disclosure. When an automated system came together some years later, it incorporated ACES checks as an integral part of its process.

By the late 1990s, PERSEREC was engaged in numerous studies related to financial prescreening and continuing assessment of security clearance holders. Among them were projects that (1) evaluated automated routines using commercial databases to identify unexplained affluence, (2) compiled guidance on how foreign intelligence services coach their agents to avoid letting their finances reveal that they are committing espionage, and how such services discern potential targets who may be vulnerable to recruitment based on financial distress, and (3) compiled government databases on finances that would be useful for CI and personnel security investigations, evaluating their usefulness, and documenting the legal and administrative restrictions on their use (Timm, 1997). From this decade of interlocking research emerged PERSEREC's first attempt to test automation on actual background investigations using a broadened menu of electronic databases in a pilot study that began in October 1998.

THE DATABASE MATCHING PILOT STUDY

The Database Matching Pilot Study evolved from requests that PERSEREC assess the feasibility of incorporating additional data sources into its system that would become ACES. The requests came from two senior DoD security officials, one interested in foreign travel databases and the other in databases holding information on arrests for various crimes. After completing preliminary research in those two areas, PERSEREC designed a broad-based study to assess the feasibility and value of procuring data from 15 untapped government and commercial databases that were not routinely checked in background investigations, including

[5] In Ames' case, the especially sensitive information to which he had access were the names of all Soviets cooperating with American intelligence agencies. These he exchanged with his Soviet handlers for cash, and 10 spies for the United States were executed as a result (U.S. Senate Select Committee on Intelligence, 1994).

immigration, criminal, court, tax, bank, driver's license, and naturalization records (Chandler, Timm, Massey, & Zimmerman, 2001).

The pilot study proceeded on two fronts: one element sent automated queries to 11 of the 15 databases (the 11 that entered into memoranda of agreement authorizing this access) and returned the results to DSS (previously DIS) to be used in 500 actual background investigations conducted from three DSS field offices in Northern California.[6] DSS investigators completed an evaluation on the value of the data returned for each case, and included the data from the automated queries in their official reports of investigation (ROI) sent to adjudicators (Chandler, et al., 2001).

The second element in the pilot study was a statistical match between all 15 of the databases and a large stratified sample of 18,000 persons who had recently undergone DSS investigations. A statistical match seeks to learn how many individuals in the sample have records that relate to them in any of the databases. Without using their identities, individuals were matched to their records using Social Security numbers. The study sampled nine subpopulations of recent clearance applicants defined by employment type (military, civilian, or contractor) and by clearance level (S, TS, and Sensitive Compartmented Information [SCI]). The goal was to determine how large the "hit rate" would be to queries of these databases to see how much useful information was likely to result for background investigations, and to estimate how much time and money would be required on the part of adjudicators to react to the information (Chandler, et al., 2001).

While the Database Matching Pilot Study proceeded in 1999, in February of that year DoD officials requested a rationale from PERSEREC outlining how automated searches of electronic databases would enhance personnel security. In the plan it submitted, PERSEREC emphasized the benefits of adding an aperiodic element that would check electronic databases on clearance holders in-between the fixed 5-year or 10-year reinvestigation period. Doing this could increase deterrence of security-relevant misbehavior because clearance holders would not know exactly when their records would be checked, and it would generate useful information closer in time

[6] Although PERSEREC provided database checks for the 500 individuals in the original sample, the actual number of cases in the study was 365. Various problems led to the loss of 135 cases from the study: in 61 cases, investigators did not return fully completed evaluation forms; other subjects moved out of state before being interviewed, or they terminated their employment, some declined to be interviewed, and others were discharged from military service during the study. In one instance, a subject was caught embezzling funds from an employer while applying for a security clearance (Chandler, et al., 2001).

to when any incidents of security concern occurred[7] ("Development of a Prototype," 1999).

In April 1999, DoD requested that PERSEREC plan to develop a prototype of an automated system. This would be a proof of concept project to build a system and demonstrate that it would work and be cost effective. The system should be capable of four actions: (1) pulling information on the subjects from each of the specific databases; (2) assessing whether the derogatory information returned by the searches exceeded established thresholds; (3) assessing when information returned should trigger an aperiodic reinvestigation; and (4) electronically forwarding results from the searches for dissemination to investigators and adjudicators ("Development of a Prototype," 1999). This initial plan already captured essential parts of the vision for ACES since, from its inception, ACES would not merely locate data about subjects, but would apply business rules to that data based on guidance from adjudicators, and having analyzed the data, electronically transfer the results in a report that would be useful to those customers.

With potential backers in the Office of the Secretary of Defense (OSD) interested in seeing ACES in action, officials there encouraged PERSEREC to fast track results from the Database Matching Pilot Study. Researchers should collect, analyze, and report on the data that could be gathered by January 31, 2000. A pre-publication draft reported results in January, and a final report was published a year later (Chandler, Timm, Massey, & Zimmerman, DRAFT, 2000; Chandler, et al., 2001).

The Database Matching Pilot Study demonstrated that an automated system for checking electronic databases could work and provided valuable information for personnel security decisions. For example, of the 18,000 persons included in the statistical match sample, ACES identified three for whom Suspicious Activity Reports (SARs) had been filed. Financial institutions file a SAR when they suspect a client of money laundering of other serious financial crime. ACES identified 36 persons who had unsuitability discharges from the military that they were not reporting. It found that 1.5% of three subsets of persons with S or TS clearances in the sample were in the Health and Human Services Tax Offset Database, meaning that they were at least $500 behind on their child support payments and were scheduled to have some or all of their federal tax refunds seized (Chandler, et al., 2001).

---

[7] John Walker's espionage during the 1970s and 80s illustrated the danger of relying only on fixed periodic reinvestigations. After establishing a profitable exchange with his Soviet handlers, divorced, and facing another 5-year reinvestigation soon, Walker resigned from the U.S. Navy rather than risk being discovered. "But after he and Barbara divorced, John felt he had no choice but to retire because he knew that he couldn't survive a background investigation and he was afraid to chance forging another one. ' It was just too risky with Barbara shooting off her mouth.'" He then continued spying as a civilian by passing on classified information he got from friends and family members who still had access. Walker's wife, Barbara, knew about his espionage and threatened to turn him in while they were still married. She eventually did so years later, resulting in his arrest (Early, 1988).

Researchers enlisted DSS investigators to evaluate the accuracy and utility of the information obtained from each new database and on each case in the Database Matching Pilot Study. They held focus groups with these investigators to understand their reasoning, in order to closely tailor their emerging system to the needs of DoD. Later, researchers surveyed adjudicators to see how useful they found each database in making their decisions. For example, investigators found the Customs Service foreign travel information useful when they could follow up in a subject interview with an applicant, and it would be especially useful for verifying travel that people self-reported and for checking passport records. For each of the databases in the study, PERSEREC collected reactions and suggestions from those doing the background investigations in the field to see if the automated data clarified or added to what they found from their usual sources, and this coordination ensured that the automated system would be closely shaped to the requirements of personnel security (Chandler, et al., 2001).

EVALUATING THE POTENTIAL IMPACT OF ACES ON ADJUDICATION

While one stream of research leading to ACES, such as the Pilot Study, evaluated available databases, another stream explored what the implications for the personnel security process would be of adding automated database checks—how many additional cases with security issues might be identified from these checks, and how would this additional data affect the numbers of personnel, their time, and the resources needed to deal with them? A study in 2000 based on completed cases from the Office of Personnel Management (OPM) addressed these questions and evaluated how many cases with serious issues (in this instance, issues that were already known from completed background investigations) the ACES checks would have caught and how many they would have missed (Timm, 2001). If ACES identified cases with serious issues as readily as investigators did, a strong case could be made for replacing the TS reinvestigations at 5-year intervals with the less expensive aperiodic ACES checks for everyone, and applying some of the resulting savings to following up with full scale investigations of the cases ACES had flagged (Timm, 2001). In a retrospective design, researchers looked at 11,065 closed OPM Periodic Reinvestigations (PRs) and compared the ROI with results derived from ACES checks on these individuals. They found that ACES offered the potential to "dramatically decrease" the number of PRs that would be triggered for investigative expansion with "practically no decrease" in the number of cases identified as having serious issues (Timm, 2001). When these early studies returned promising results, OSD encouraged PERSEREC's staff to continue developing ACES for eventual implementation across DoD.

RESEARCH ON PRODUCTIVITY OF INVESTIGATIVE SOURCES: ITS IMPACT ON ACES

At the same time that ACES was being developed, other researchers at PERSEREC were working on a series of studies that compared the various sources consulted in

a periodic reinvestigation (a Single-Scope Background Investigation-Periodic Reinvestigation [SSBI-PR]) to determine how productive they were. This research also influenced development of ACES. Federal Investigative Standards (FIS) specified which records must be checked and which persons should be interviewed during an investigation. A source is "productive" if it yields the type of information that is being sought. In the case of a background investigation for a security clearance, this means information that suggests potential concerns relating to one or more of the 13 Adjudicative Guidelines, such as financial problems, criminal behaviors, or unreported foreign contacts. The productivity of sources studies done in 2001 demonstrated that just three of these sources, SF-86 (the security questionnaire filled out by the applicant), the interview of the applicant, and the checks of the applicant's credit records, identified almost all potential cases with security issues, and they identified every single instance in which one of the four agencies in the study took an administrative action to revoke or deny a clearance (Kramer, Crawford, Heuer, Jr., & Hagen, 2001; Buck, 2010). The three most productive sources also were among the most inexpensive, while the costly activities, such as interviewing neighbors or co-workers, yielded the least relevant information.

Based on these results from the productivity of sources research, PERSEREC proposed and secured a major change in federal standards for background reinvestigations. The most productive and least expensive sources should be consulted first in a Phase One of the SSBI-PR: the SF-86, the subject interview, and the credit bureau checks. If the Phase One activities turned up no security issues, PERSEREC research demonstrated that in virtually every instance that case was clean and required no additional investigative activities. If security issues were found during Phase One, then the rest of the investigative activities could be performed in Phase Two to expand the scrutiny. Adopting this Phased Periodic Reinvestigation for TS investigations would save millions of dollars that could be shifted to implementing regular but a-periodic ACES checks of electronic databases annually or in-between the 5-year intervals for reinvestigation. The federal government would get more for its money by investing first in the most productive sources in a reinvestigation, doing the more expensive steps only on the relatively few cases that had security issues, and applying the savings to a program of ACES monitoring (Heuer, Jr., Crawford, Kramer, & Hagen, 2001). Proof that specific sources were more productive and others less so, and that no security issues were missed by relying on the most productive sources, prompted officials in 2005 to adopt the Phased Periodic Reinvestigation as an option across the government (Information Security Oversight Office, 2004). This would later influence the decision of security policy officials to build automated records checks (ARCs) into a new reformed personnel security process.

The findings of the productivity of sources research strengthened the case for adopting ARC (such as ACES) into the personnel security process, and focused the case on several capabilities. First, doing annual or a-periodic ARC in-between

periodic reinvestigations would avoid the predictable scheduling of the 5-year reinvestigation and prevent clearance holders taking advantage of a 5-year window of opportunity to misbehave. Second, generating savings from the efficiencies of the Phased Periodic Reinvestigation could be used to implement ACES across agencies. More consistent and effective monitoring to recognize and respond to security issues sooner became possible with the combination of the Phased Periodic Reinvestigation and ARC such as ACES.

DEVELOPING ACES VERSION ONE

Encouraged by the results of the Database Matching Pilot Study and the productivity of sources research, in February 2002 PERSEREC researchers published the *ACES Program Management Plan and Concept of Operations (CONOPS)* (Chandler & Timm, 2002) describing how a mature ACES could support DoD's personnel security program. Much of this plan, which assumed DoD backing and funding for a system scaled to support adjudicators at the eight Central Adjudication Facilities (CAFs), who would be checking records on thousands of individuals each day, was not immediately implemented. The initial investment ACES required was not available at that time.

Research also showed that further enhancements to the system, such as the addition of the National Law Enforcement Telecommunications System (NLETS) checks, were needed. Instead of developing ACES as a DoD entity, as the CONOPS outlined, PERSEREC undertook research and demonstration projects for agencies including the Department of Homeland Security (DHS) and the DSS while at the same time system enhancements like NLETS were added. These studies evaluated the value and feasibility of checking additional databases and expanding the ACES routines. The initial software and programming that had been used in the early pilot studies were iteratively upgraded to be able to handle a larger caseload in the future in a stable production mode.

FIRST PILOTS USING "LIVE DATA": 2002 THROUGH 2005

ACES development proceeded through a series of pilot studies. Development has been incremental, building systematically on the results and revisions from each previous pilot study; it has been practical, seeking and incorporating feedback from potential users at each step in order to maximize the program's usefulness; and it has been pragmatic, responding to new customers as their interest and funding allowed. Descriptions of the major ACES pilot projects can be found in APPENDIX A.

Two pilot studies shaped the development of Version One of ACES: the first started in early 2002 and ended mid-2003; the second began in 2004 and ended in late 2005. In the 2002 pilot study, PERSEREC conducted ACES checks on 14,000 individuals with Air Force TS or SCI access. This was the first ACES pilot study to use "live" data, not retrospective data from completed cases, and the first to refer cases of security concern that it identified to an adjudicative authority, either the Air Force CAF (AFCAF), or the Defense Intelligence Agency (DIA) for adjudicator follow-up (Chandler, 2002) .

Early results in 2002 showed that checks were conducted on some Air Force personnel who no longer held a clearance, so ACES processing was halted until additional data sources were incorporated to help filter out persons who had separated from the military. In April 2002, officials from all eight CAFs and from the

OSD attended a user requirements workshop with PERSEREC to discuss the business rules that ACES would apply to cases, the means of data transmittal to the CAFs, and the content and style of the reports ACES would transmit (Chandler, 2002; Rome, Jr., & Chandler, 2005).

These business rules were usually expressed in the form of "if—then" statements. For example, a rule on personal conduct might include the following:[8]

> ACES shall identify if the subject's clearance or access from a Federal agency outside the DoD was terminated for cause, and the matter was not reported on the subject's prior Personnel Security Questionnaire. (Chandler, 2006).

The group's suggestions led to major modifications of the business rules that would identify new cases with potential security issues ("issue cases" in short) and to the ACES reports. OSD officials requested that these changes be implemented in ACES before processing of cases in the pilot study resumed, and it was July before another batch of 9,700 cases ran using the revised rules. Results showed that ACES identified 9.31% of subjects as issue cases under the revised rules. This proved too fine a net. Adjudicators reported that too many minor issues were included under those rules, so in January 2003, following the pilot study, further refinement of the financial thresholds reduced the number of issue cases identified to roughly 5%. As a result, the CAFs would receive far fewer cases that would be of only marginal interest to them (Rome, Jr., & Chandler, 2005).

The second pilot study leading to Version One of ACES was called the ACES Beta Test. It began in August 2004. It used the same databases as in the 2002 pilot study, but the sample was drawn from individuals holding TS or SCI access under the jurisdiction of seven of the eight DoD CAFs. Subjects were at the midpoint before their next 5-year reinvestigations were due.[9] Researchers selected at least 1,500 individuals from each CAF in five batches, 12,710 individuals in all. In order to space out the workload for the adjudicators who would need to review and respond to the results, researchers sequenced running the batches and sending the report of results to each CAF by Compact Disc Read-only Memory (CD-ROM) as a batch was completed at several-week intervals (Rome, Jr., & Chandler, 2005).

Results from this 2004 ACES Beta Test demonstrated that ACES successfully identified new information that adjudicators were concerned about in 80% of the cases, and in one-fourth of those cases further action was taken, indicating that the issues were serious. ACES found problems that investigators and other sources had not previously identified. For example, ACES identified one person with tax liens

---

[8] Thresholds and sources for this business rule are deleted in this example.

[9] The eight CAFs included Air Force CAF (AFCAF), DIA CAF, Department of the Navy and Marines (DON) CAF, Defense Industrial Security Clearance Office (DISCO), Army Central Clearance Facility (CCF), Washington Headquarters Service (WHS) CAF, Joint Chiefs of Staff (JCS) CAF, and the Defense Office of Hearings and Appeals (DOHA).

exceeding $185,000 (indicating indebtedness), another person with a positive drug test for amphetamines (indicating drug use and unreliability), and someone with arrests for multiple felonies (including abuse and assault). Adjudicators completed evaluation forms on the ACES data they received, and this feedback guided further revisions to next iterations of the system. The financial business rules were adjusted according to adjudicator's suggestions in 2005 (Rome, Jr., & Chandler, 2005).

During the 4 years, work on Version One proceeded while ACES checks were being conducted for different agencies, testing new uses, improving interfaces to important databases, and further demonstrating ACES' effectiveness at identifying issues of security and counterintelligence concern. These efforts included: (1) testing further automation of NLETS to obtain criminal history records from state repositories; (2) exploring how leads generated in ACES would be useful to CI units; (3) applying ACES to a new population in a pilot study with DHS; and (4) comparing ACES results to the those from background investigations (Rome, Jr., & Chandler, 2005; Timm, Buck, & Chandler, 2004; Chandler & Jung, 2007; Richmond, Chandler, & Jung, 2008).

TECHNICAL AND OPERATIONAL DESCRIPTION OF ACES VERSION ONE

Since ACES constantly evolved to align with the needs of the various agencies that sponsored its development, describing it at one point in time does not capture what it had earlier been or what it would become. Nevertheless, the set of features in Version One before 2009 became known as the "legacy system"; this describes the computer resources on which the legacy system relied and how it worked.

Operational Policies and Constraints

The first thing to remember in understanding how any version of ACES works is that there are legal and policy restrictions on who can be considered for an ACES check, which data repositories can be checked, and on the distribution, control, and use of the information gathered through ACES checks.

Initially, the eligible population was limited to specific types of individuals: military personnel, DoD employees, and DoD civilian contractors. Later, most of the data use agreements were expanded to include individuals who require either (1) a security clearance with the federal government, (2) suitability screening for government employment, or (3) logical access to a government network or physical access to a government facility. The appropriate use of information resulting from an ACES check includes background investigations, CI investigations, and adjudications related to suitability or security clearances.

Moreover, the information resulting from an ACES check must be protected in accordance with the provisions of the Privacy Act of 1974. Thus, ACES data and ACES reports cannot be disclosed, discussed, or shared with individuals unless they have a need-to-know in the performance of their official duties. Appropriate

physical security, information assurance, and personnel security safeguards must be used to prevent unauthorized access to ACES data and ACES reports.

Inputs, Processing, and Outputs of ACES

ACES Version One obtained data from a wide range of sources, merged that data, and then used it to identify issues of security concern. It then produced reports on individuals that (1) summarized those issues, and (2) provided all of the detailed information that was collected on the individual. These reports were sent to adjudicators at the CAFs to assist them in making determinations regarding whether individuals would be granted or would continue in access to sensitive information. A nominal fee was charged for each report.

Each ACES check is focused on concerns in the 13 Uniform Adjudicative Guidelines, the latest version of which was adopted in 2005. The guidelines specify areas of conduct that could endanger the protection of sensitive information. (Hadley, 2005) They include:

- 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
- Handling Protected Information
- Outside Activities
- Use of Information Technology Systems

ACES Version One collected information from numerous systems of other government and commercial entities to receive its data. There were three types of interactions. Some were computer-to-computer and were fully automated. For others, the interactions were indirect. In those indirect interactions, a request file was burned to a Compact Disc (CD) and sent to the external entity (usually via FedEx), where it was manually uploaded to the system (usually a mainframe computer), and a job was submitted asking to retrieve data for the individuals in the request file. The files produced by the job were then burned to a CD and sent back to PERSEREC, where the ACES Operator ran a computer program to load the data into the ACES database. The third and most common type of interaction was computer-to-computer but with some manual intervention required by the ACES

Operator. For example, the transfer of files between systems might be fully automated, but when the response files were received, the ACES Operator needed to run a computer program to load the data into the database. There were no instances in which requests or responses were created in hardcopy and then manually scanned or keyed into a computer.

Legacy System Components

The ACES Version One production system consisted of Commercial Off-The-Shelf (COTS) software as well as custom software. The system initially ran on a Digital Equipment Corporation Alphaserver running Windows, and was later migrated to Sun Microsystems hardware running the Solaris UNIX operating system. The core system consisted of a database server running Oracle relational database software. Dedicated circuits were added to establish secure connections to the National Crime Information Center (NCIC), and to NLETS. A separate external interface server handled the interfaces to other external systems, such as the credit bureaus. Finally, a separate application server was used to run the Java software that produced the ACES reports.

In Figure 1, a high-level depiction of the ACES Version One system components and their relationship to data providers illustrates the system.

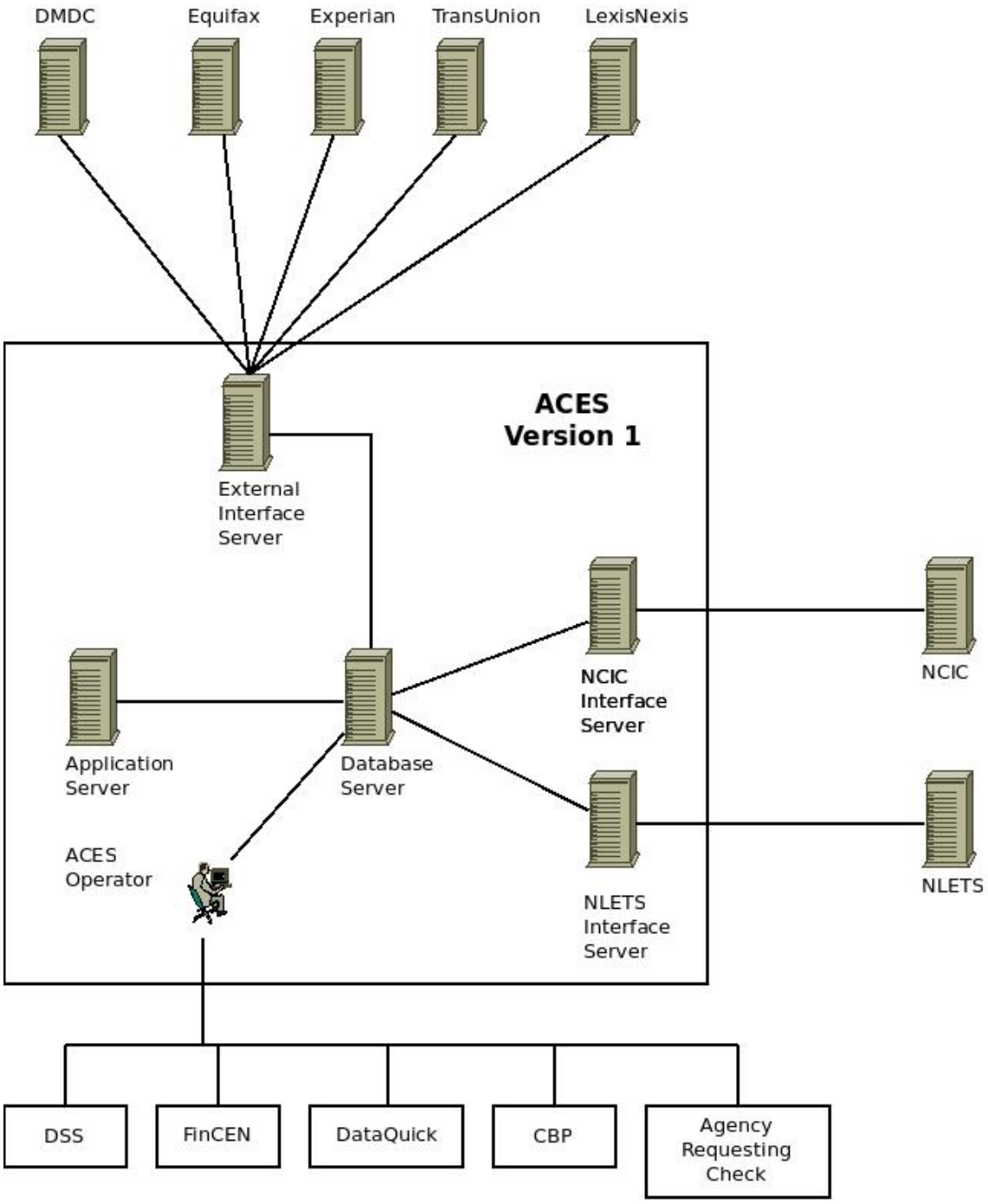

Figure 1 High-Level View of Version One of the ACES System

Figure 1 illustrates the different modes of transmitting information to and from external data providers, either computer-to-computer or manual. For example, the check of DMDC records used file transfer software to move files between the ACES Database Server and the External Interface Server, and between the ACES External Interface Server and the DMDC Server. On the other hand, the FinCEN check was a more indirect manual process in which the ACES Operator copied the inquiry file from the ACES Database Server, and then emailed it to a contact at FinCEN. The

file was uploaded to the FinCEN computer, where it was processed. When the processing was completed, the response files were downloaded at FinCEN and emailed to the ACES Operator, who transferred them to the ACES Database Server. The system capabilities of the various data providers and the nature of their electronic files and resources dictated this variety of approaches.

Capacity and Performance

Version One of ACES was capable of initiating 5,000 checks per week. Since it took approximately 24 to 26 days to complete one batch of ACES checks, ACES Version One suffered from performance limitations. The capabilities of the hardware platform produced some of these limitations, while others were due to an aging software architecture. However, by far the longest time lags in conducting ACES checks with Version One came from some of the external data providers, such as DMDC and FinCEN. These external interfaces required manual steps to transfer requests and data between ACES and the providers. In addition, initially these providers did not offer automated processes for filling data requests from ACES. The resulting time lags could be several days or, in some cases, several weeks. Later DMDC and FinCEN provided a more automated interface and ACES checks could be run within 24 hours.

Physical Security and Data Privacy Protections

The ACES security and privacy protections met DoD policy requirements. The facilities at PERSEREC, where ACES Version One was hosted, were alarmed and actively monitored remotely. There were cipher locks on all external doors, and sprinkler systems in every building. In addition, there were special cipher locks on the computing facility, and the combination was only given to personnel who needed access to the facility for their employment.

All personnel requiring access to the ACES system (in Version One as well as in later versions) or its data (1) held a TS clearance, based on a Single Scope Background Investigation (SSBI), or (2) were granted an interim access to TS information while waiting for the results of their SSBI. In addition, such personnel receive periodic security awareness training, training in safeguarding Privacy Act data, and training in handling law enforcement sensitive data. Access to the ACES database was monitored. Any time a record was inserted, modified, or deleted in a database, that action was recorded in a separate area of the database that could only be viewed by authorized personnel.

Information Assurance Protections

Backups of the ACES data and software were performed at regular intervals. Copies of the backup tapes were housed off-site at a secure facility. When no longer needed, hard drives and other media that once contained PII were destroyed in accordance with DoD regulations. Similarly, printouts of ACES reports or other paper copy containing PII data were shredded by a bonded contractor.

Modes of Operation

ACES Version One operated during regular business hours on weekdays. Checks were performed a-periodically as organizations requested and paid for them. Although the system was automated, in the sense that there was no manual data entry and all the data processing and report production were performed by computer, the system still required a human operator. The tasks performed by the ACES Operator included:

- Initiating certain software processes (e.g., to load data into the database);
- Verifying the results of certain software processes (e.g., that the data were loaded without errors);
- Manually transferring request files to certain data providers;
- Manually transferring response files from certain data providers; and
- Taking corrective actions when errors occurred.

From the perspective of the agencies requesting ACES checks, they made requests and received reports back without having direct access to ACES. Version One did not become an operational DoD system agency-wide. Use of the system was limited to pilot testing by DoD and DHS components.

User Classes and Other Involved Personnel

Users of ACES Version One included adjudicators working at DoD CAFs and at similar adjudication facilities in other branches of the federal government. These individuals simply received computer files, in HyperText Markup Language (HTML) format, which were sent to the CAF via the case management software developed by the U.S. Air Force or via the OPM Secure Portal. The ACES Operator, developers, analysts, quality assurance personnel, and a limited group of researchers at PERSEREC had access to the system.

THE IMPACT OF PERSONNEL SECURITY REFORMS ON ACES

As ACES Version One developed the technology and linkages to smoothly conduct automated checks of a suite of electronic records, events were changing the context of personnel security in ways that would highlight ACES capabilities. The inefficiencies in the federal personnel security system had been the target of reformers for decades, but the terrorist attack of September 11, 2001, sharply focused reform efforts. The attack produced a flood of additional security clearance requests that threatened to overwhelm the personnel security system as it drove up the backlog of overdue clearance decisions. Congress responded by passing the Intelligence Reform and Terrorist Prevention Act (IRTPA) in December 2004, which, among other reforms, mandated specific timelines for completing federal background investigations and adjudications. In 2005, the Government Accountability Office (GAO), which had been critical of the security clearance process for years, placed DoD's personnel security system on its High Risk List, which meant the GAO would closely monitor DoD's efforts to improve until GAO evaluators were satisfied their concerns had been met (Government Accountability Office, 2005).[10]

These two milestones—IRTPA and the High-Risk designation by the GAO— prodded serious efforts to coordinate government-wide reform of the personnel security system. In June 2007, the Joint Security Process Reform Team was formed by a memorandum of agreement between DoD and the Office of the Director of National Intelligence (ODNI) (Government Accountability Office, 2012). Further restructuring by the President in E.O. 13467 in June 2008 expanded the reform team to include the Office of Management and Budget (OMB) and OPM in the Joint Suitability and Security Reform Team, soon shortened to Joint Reform Team and eventually to the current name, the Joint Reform Effort (JRE). The E.O. created a Performance Accountability Council (PAC) headed by OMB to oversee the reform effort, and two executive agents, the Security Executive in charge of security clearance reform, and the Suitability Executive in charge of reforming suitability, i.e., the evaluation of fitness for federal employment. The ODNI was appointed Security Executive, and the Director of OPM was appointed Suitability Executive (Government Accountability Office, 2012). With this structure, reform of federal personnel security proceeded over the next 5 years.

Because ACES was already a successful and functioning automated system for checking security-related records, it was selected for use in efforts to explore reform of the federal personnel security process. PERSEREC began to plan for a broader application of ACES beyond DoD based on the newly adopted Phased SSBI-PR. Officials suggested to the JRE team that ACES checks plus SF-86 responses, checks of FBI and local law enforcement records and appropriate case expansion

[10] GAO removed the DoD security clearance program from the High-Risk List in January 2011(Government Accountability Office, 2012).

could, without a loss of security, replace the regular 5-year SSBI-PR for agencies across the federal government, saving time and millions of dollars (Chandler, 2008). Projections for how ACES could develop in the future envisioned that (1) it could replace the manual checking of records by investigators during initial SSBIs, (2) ACES would run ad hoc records checks whenever a clearance holder's behavior raised a new security issue, and (3) ACES would send alerts in real time to notify adjudicators when ACES identified a new security issue for an individual (Chandler, 2008).

In the 2008 version of the revised FIS, the JRE restructured the steps traditionally performed in the background investigation process in order to improve efficiency and take advantage of automation. In the new process, more information would be collected and validated in early steps using an expanded electronic application and ARC of electronic databases using an automated system such as ACES. Next, automated business rules would scan the information that had been collected for issues, flag any issues of security concern identified, and electronically adjudicate (eAdjudicate) cases to make a risk assessment decision (Joint Suitability and Security Reform Team, 2008a). Clean cases—those without flagged issues—would need no further human handling. Only then, if necessary, an investigator would interview the applicant about the issues that had already been identified with flags. These steps built on PERSEREC's research on productivity of sources and phasing of the investigation. Further issues that remained unresolved after the subject interview would be addressed by investigators making phone calls and visiting records repositories in the traditional way. This revision reflected the fact that the interview and the investigators' activities are the most expensive and time-consuming parts of the investigation, so inexpensive automated checks should be performed first to guide the interview and the investigators to focus on the actual issues of the case, if there were any. The FIS were further revised and signed, but not implemented, in 2012 (Chandler & Timm, 2009).

When the JRE made ARC one of the essential components of the restructured federal strategy for personnel security investigation, it catapulted the ACES program from a DoD-focused capability into a national asset. Starting in 2008, the direction of ACES research and development shifted to reflect the goals of the JRE and the emerging national program. ACES researchers undertook a series of pilot studies for various federal agencies to demonstrate ACES' capabilities in various types of investigations, in various experimental conditions, in comparison with ARC capabilities of other agencies, and compared with traditional investigations by various providers. These ACES pilot studies proved that a flagging strategy, relying on automated database checks to identify and "flag" any potential issues that could then be followed up on by an investigator, identified issues to the risk management

standards that were agreed to across agencies (Joint Suitability and Security Reform Team, 2008b).[11]

[11] The flagging strategy built on earlier PERSEREC research on productivity of sources and the related Phased Periodic Reinvestigation, since any issue identified in early steps would be flagged and followed up in later investigative steps performed because of the presence of flags, or issues of security concern already identified.

DEVELOPING ACES VERSION TWO

The JRE's new vision for ARC prompted the need to revise and expand the ACES system. ACES was no longer limited to the role of continuous evaluation (CE) but was being considered for integration into the initial background investigation, and it would reach beyond DoD personnel and contractors to a wider population, to include other departments of the federal government. Its automated checks would apply not only to individuals with TS and SCI access, but also to those seeking an S clearance and to positions of trust that do not require a security clearance. Program sponsors also requested some new features that would need to be added to the ACES system, such as a la carte checks and a Web Service Interface. These changes in how ACES would be applied meant the system would be dealing with a greatly expanded scope and the volume of checks would increase exponentially (Zimmerman & Chandler, 2010).[12]

TECHNICAL AND OPERATIONAL DESCRIPTION OF ACES VERSION TWO

System Attributes

Version Two was planned to be able to process two million cases per year, but has evolved to be scalable up to five million per year. ACES would need to take advantage of newer technologies that had developed or matured since the development of the ACES Version One, including:

- Infrastructure independence: System functions on different hardware and software platforms to mitigate the negative consequences of relying exclusively on particular vendors.
- Modularity: Each major function or external interface is designed as a separate software component, separated by logical boundaries, with a clearly defined interface for communicating with the component.
- Loose coupling: Major software components should be replaceable without affecting other components of the system.
- Scalability: Accommodates an increased volume of ACES checks.
- Extensibility: Allows for incorporation of new types of checks in the future.
- Comprehensiveness: Provides support for lifecycle management processes.
- Flexibility: System will meet the changing needs of users.

Additional sources of electronic records were added to Version Two to improve verification of identity, education, and employment. New network and new software architectures were developed to move the bulk of the processing from the database server to an application server. The external interfaces between ACES and the data

[12] The following section is based on the draft Concept of Operations by Zimmerman and Chandler, 2010.

providers were improved to increase automation and reduce the operational role of the ACES Operator, who would become a monitor of the system, intervening only when necessary. The procurement of more powerful hardware, as well as these software changes, led to improving the speed of external interfaces to data providers and to faster processing of records, and it increased the number of cases the system could store.

A new Web Services Interface was developed that works through a machine-to-machine interface to allow user agencies to directly request checks and download reports across the Internet.

Operational Policies and Constraints

In ACES Version Two, as in the earlier version, the restrictions continued on who could be considered for an ACES check as well as on the distribution, control, and use of information provided by an ACES check. The eligible population for ACES checks remained military personnel, employees of the federal government, civilian contractors working for the federal government, but added to those were persons who required background investigations to fulfill Homeland Security Presidential Directive-12 (HSPD-12) requirements.

The information resulting from an ACES check remained subject to the Privacy Act of 1974. Thus, ACES data and ACES reports could not be disclosed, discussed, or shared with individuals unless they had a direct need-to-know in the performance of their official duties. Physical and logical safeguards applied to ACES continued to meet DoD security requirements. In addition, external data providers imposed further constraints. These constraints were specified in agreements, contracts, and policies.

Since Version Two allows user agencies to access the ACES system directly to request ACES checks and to obtain reports via the Web Services Interface, new policies and procedures were required. An ACES Web Services Interface Control Document outlines the procedures that agencies requiring such access should follow, and these agencies completed a formal agreement with the operating agency for ACES. Responsibility for the development, operations, and maintenance of the system was envisioned by the JRE to transition to the Defense Information Systems for Security (DISS) Family of Systems. Currently, PERSEREC continues to operate ACES for pilot studies and research.

Inputs, Processing, and Outputs of ACES Version Two

In order to increase the capabilities of ACES so that checks could be performed more quickly and on larger numbers of people, the hardware platform was upgraded, the software architecture was reconfigured, and the role of the ACES Operator was simplified through automation, especially for handling the external interfaces. Figure 2 provides a high-level view of how ACES Version Two relates to

its data sources, to other system inputs, and to individuals or organizations that receive system outputs.

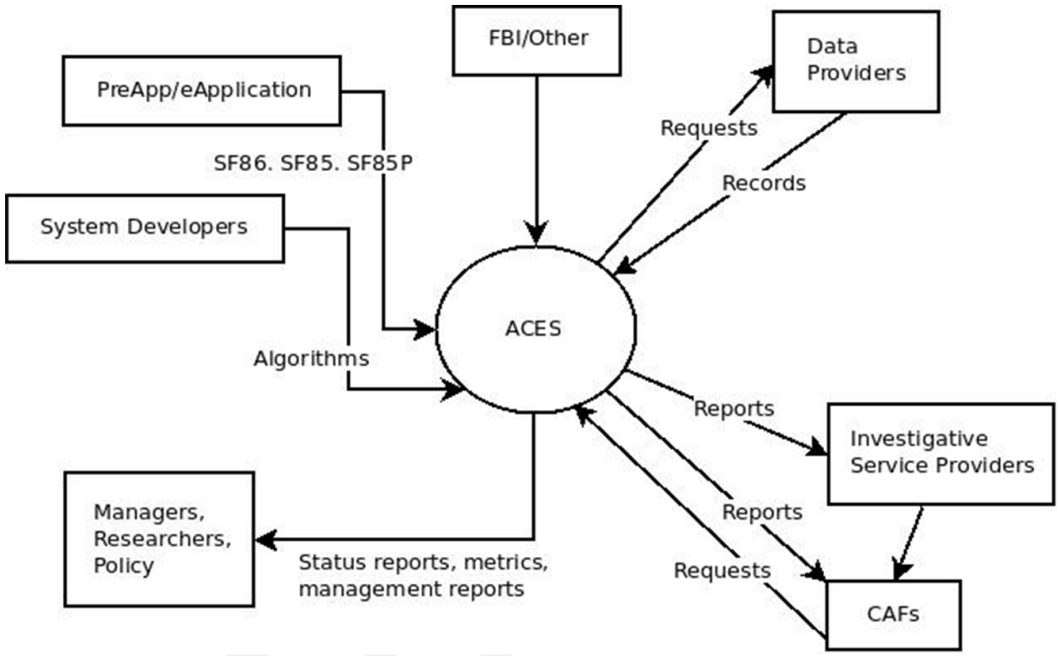

Figure 2 High-Level View of ACES Inputs and Outputs

As the figure shows, ACES Version Two may receive data inputs from various sources, including:

- Completed Personnel Security Questionnaires (e.g., SF-86 or Standard Form 85 [SF-85]);
- FBI and other criminal history data sources;
- Other data providers (e.g., LexisNexis, DMDC).

System developers refined the software that applies the algorithms for identifying security-relevant issues in the data. Information in the ACES reports, based on ACES checks, is provided to the DoD CAFs and to Investigation Service Providers (ISPs) to guide their activities. In addition, aggregated information derived from the data, and from information about the usage and performance of the system itself, is provided to managers, researchers, and policy officials.

Tiered processing to reflect the revised FIS, which mandate a hierarchy of tiers for background investigations, could be included in Version Two of the ACES system when a final version of the standards is implemented.[13] A new set of standardized management reports would also greatly enhance the operation of the system. Management reports are important tools for monitoring the status of operations, for

[13] As of September 2013, the revised Federal Investigative Standards had been approved, but not implemented.

cost accounting and budgeting, and for quality control. Requirements have been developed for eight different management reports as well as a user interface for generating them.

System Components

Currently, ACES Version Two is comprised of COTS as well as custom Java and Oracle Procedural Language/Structured Query Language (PL/SQL) software running on Sun Microsystems servers. The system is running on the Solaris operating system, Oracle relational database software, Oracle Application Server software, OpenSSH client and server software, and Connect:Direct file transfer software. Figure 3 provides a high-level depiction of the ACES Version Two system components and their interactions with data providers.

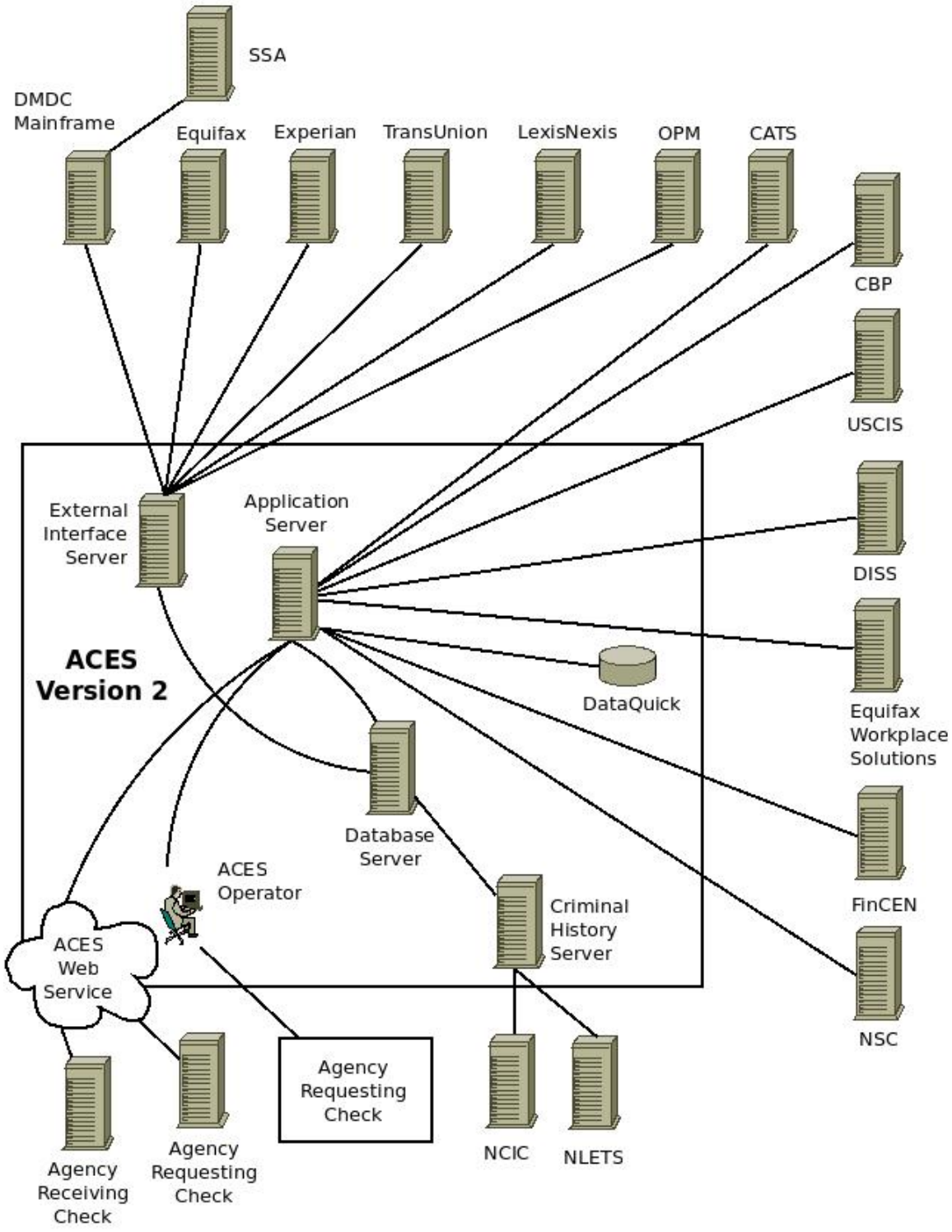

Figure 3 High-Level View of Version Two of the ACES System

In ACES Version Two, many of the transmissions to and from external data providers employ computer-to-computer interfaces; some are batch processes. Figure 3 displays the computer-to-computer interfaces that handle requests for

ACES checks and the distribution of ACES reports. The figure depicts two options for how agencies request ACES checks: (1) using the ACES Web Service, or (2) various other means, including submitting requests by encrypted email, or encrypted files via CD, or file transfers such as the Secure File Transfer Protocol (SFTP), Connect:Direct, or the portal offered by OPM.

THE CONTEXT FOR ACES IN THE DOD

The work of the JRE (in which the DoD is one of the four participating agencies) over the last 5 years has been an important influence on ACES because the JRE adopted ARC as one of the seven essential steps in its vision for an automated personnel security process, and ACES is one example of an ARC system. The scope of ACES development expanded as a result of this influence to address the requirements for ARC in other types of background investigations and to meet the needs of additional federal agencies, which necessitated the updated and expanded ACES Version Two.

Changes in organizational context within DoD were a second important influence on ACES. Improving the DoD personnel security program had been a perennial concern in the department for decades, but starting in 2004 and 2005, in response to criticism such as that in IRTPA and by the GAO, DoD entered an extended period of upheaval as it repeatedly changed the authorities over the various personnel security processes, seeking success. Since DoD had supported and sponsored ACES from its beginnings, organizational perturbation affected ACES' development. During this upheaval, two changes in DoD especially influenced ACES: (1) the transfer of DoD's background investigations to OPM in 2005, and (2) the creation of DISS in 2009.

In January 2003, DoD decided to stop doing background investigations on applicants for DoD security clearances, and entered into negotiations with OPM to purchase that service. The transfer took some time because it forced OPM to expand its investigator workforce and its scale of operations, but in February 2005, the transfer of DoD's investigative functions from DSS, along with most of the DSS government investigators, to OPM was completed (Memorandum of Agreement, 2004). After several more years of adjustment, by 2009 OPM could claim to be meeting most of the IRTPA goals for timeliness of its DoD investigations.

This shift of responsibility for investigations affected ACES because it had originally been built as a DoD system for CE to support DoD investigations and adjudicative decisions. As the JRE advanced its plans to systematize personnel security functions to interact with and be consistent across federal agencies, the team's ARC step assumed that the provider of investigations (increasingly this was OPM as it came to perform over 90% of federal investigations) and the provider of ARC (DoD's ACES) could and would work in close coordination. This coordination proved more elusive than had been anticipated; the necessity to compromise with OPM's methods and dated technology slowed progress and added additional phases of research to ACES development.

In order to achieve the level of information technology needed to perform JRE's vision of an automated personnel security process, DISS was created under the

Business Transformation Agency (BTA) in 2009.[14] DISS' task was to plan and implement the JRE's vision in DoD, an "enterprise capability," shifting the clearance systems, processes, and supporting Information Technology (IT) systems in various DoD agencies to one standard that would be interoperable across the government. They defined their mission as one of assuming JRE's vision for the future:

> [to] improve timeliness, reciprocity, quality and cost efficiencies though design and implementation of secure, end-to-end IT capabilities. This system shall electronically collect, review and share relevant data government-wide as mandated by the Intelligence Reform and Terrorist Prevention act (IRTPA) and [other relevant authorities] (Joint Security and Suitability Reform Team, 2010; Defense Business Systems Acquisition Executive (DBSAE), 2010).

The DISS Program Management Office (PMO) continues to work toward this. Among other activities, it is guiding consolidation of the DoD CAFs (Joint Security and Suitability Reform Team, 2008b; DISS status update, 2012, DISS update for CAF consolidation meeting, 2012). Because ACES became an important element in the vision for a reformed personnel security process, DISS became the primary sponsor of ACES development. Becoming a national asset has meant ACES program management was negotiating with more players, and was repeatedly asked to demonstrate ACES' capabilities to potential customers and critics.

On the other hand, as a national asset, the ACES program has had opportunities to expand into new roles. Development of ACES in the recent past has advanced through a series of pilot projects mandated in the JRE's strategic framework. The pilot studies have been designed to test and demonstrate ACES' capabilities to perform ARC and CE. ACES has informed the strategic direction of personnel security by demonstrating that CE and ARC can be conducted in a reliable and cost effective manner to improve detection of security relevant information.

For example, the DoD/ODNI ACES Pilot Study, that began in May 2011, tested whether existing automated systems could be linked together to perform "end-to-end" electronic processing moving from submission of a clearance application to recording the adjudication decision. In this pilot study, PERSEREC worked with the ODNI, the BTA, United States Army Recruiting Command (USAREC), Omniplex, DMDC, and the Army CCF to establish legal agreements and electronic interfaces. Applications for S clearances (1,500) came from 13 USAREC stations. An S clearance requires an investigation called a National Agency Check with Local Agency Checks (NACLC). The pilot study coordinated various government and commercial organizations. Existing automated systems or processes involved in

[14] The BTA, established in 2005, in turn was disestablished as of June 2011 and many of its programs were transferred to various other DoD agencies. DISS went to the Defense Logistics Agency (DLA).

investigations or adjudications were integrated to test the end-to-end (E2E) electronic process. Among the organizations directly involved in the pilot study's investigative or adjudicative activities were:

- USAREC submitted applicants for investigation. Applicants used USAREC's Army Recruiting Information Support System electronic application (eAPP) to complete the SF-86.
- Biometrics Information Management Agency (BIMA) received fingerprints electronically and forwarded them to the FBI for a National Criminal History Check (NCHC). Livescan was used to capture and transmit fingerprints.
- Accurate Biometrics, a commercial Livescan fingerprinting provider, also received fingerprints electronically and forwarded them to the FBI for an NCHC.
- The Federal Investigative Services Division of OPM (OPM-FIS) also received fingerprints and forwarded them to the FBI for an NCHC.
- Omniplex, a contract investigative agency, conducted field investigative work and compiled the final ROI. Omniplex managed the cases using their automated case management system called the Investigative Resource Management Application (IRMA™).
- The National Reconnaissance Office (NRO) provided investigative credentials and served as the Omniplex contract owner for the pilot study; they conducted the National Agency Check (NAC) portion of the investigation. Completion of the NAC involved some manual intervention (e.g., inquiries were keyed into a computer terminal).
- PERSEREC conducted and provided ACES checks for each case.
- Army CCF received and adjudicated each completed case, using the Case Adjudications Tracking System (CATS), into which ROIs had been ingested. Adjudicative results were entered into CATS and transferred to the Joint Personnel Adjudication System (JPAS) (Ainslie, Helton-Fauth & Chandler, 2012).

Results of the pilot study encouraged prospects for moving to a completely electronic system. The average time to complete all the investigations in the pilot study was just under 24 days, surpassing the IRTPA's timeliness goal of 40 days. Without relying on fingerprint records or other agency checks, ACES by itself identified most of the cases with issues, and identified more than half of the issues in the follow-up special investigations with a subject interview. Adjudicators reported very positive feedback to the pilot study, with their time to adjudicate cases cut in half by the improved ROI. ACES checks identified actionable issues, such as unreported employment, and adjudicators felt that the array of ACES sources gave a better "whole-person" view of the subject (Ainslie, Helton-Fauth & Chandler, 2012). Based on the pilot study, PERSEREC offered DoD and the JRE a series of recommendations capitalizing on these promising results, including incorporating ACES-based ARC investigations into the accessions process and

studying the cost-avoidance implications of implementing the electronic processes on a larger scale. This and other recommendations would continue to improve the process and cut the time and money required (Ainslie, Helton-Fauth & Chandler, 2012).

By the end of 2011, in addition to completing the DoD/ODNI Pilot Study, PERSEREC was working on additional pilot studies that advanced the JRE's vision. PERSEREC and OPM were comparing the leads each brought to the then-Tier 3 of the Draft FIS, the tier for TS and SCI clearances, using a sample of Navy investigations. Another 2012 pilot study focused on DoD CE procedures in cooperation with another intelligence community partner using 2,500 cleared contractors. A feasibility analysis in 2012 evaluated two additional data sources for possible integration into ACES. Two CE projects with the Army were conducted starting in mid-2012. A pilot study with the Department of State (DoS) started in 2013 with 1,200 recently closed SSBI investigations to compare the cost and the productivity of including ACES checks in the DoS investigative process. (Chandler, 2012; F.M. Ainslie, personal communication, May 2, 2013).

Despite the lingering impact of the 2008 recession, which reduced funding across the government for research and development of efficiencies like ACES, the obvious promise of ACES continues. The current version is ACES Version 2.4, which can process the 2010 Electronic Questionnaire for Investigations Processing (e-QIP), the latest version of electronic application used by OPM in most background investigations. Future enhancements to ACES will take advantage of the availability of funds. These enhancements could include completion of re-engineering, further automation of interfaces, additional management reports, incorporation of additional data sources, and real or near-real time identification and notification of issues (Chandler, 2012).

Repeated demonstrations in various agencies and with various types of investigations have proven that ACES will streamline the expensive security clearance and suitability vetting process and greatly reduce its cost. ACES electronic database checks can be used between an initial background investigation and a periodic reinvestigation, during the career of a clearance-holder between regular reinvestigations, as a replacement for elements of the initial investigation or the reinvestigation, as a tool for prescreening military recruits, and as a tool for CI investigations. From its beginnings, the promise of ACES for the future of personnel security has been its ability to harness the power of automation to reduce costs, improve timeliness, and expand the range of information available to those who seek reliable, loyal, and trustworthy personnel.

REFERENCES

Ainslie, F. M., Helton-Fauth, W. B., & Chandler, C. J. (2012). *Department of Defense/ Director of National Intelligence Automated Continuing Evaluation System (ACES)—Pilot evaluation*. (Working Paper 12-02). Monterey, CA: Defense Personnel Security Research Center.

Buck, K. R. (2010). *Productivity of sources in background investigations for security and suitability* (MR-10-01) (FOUO). Monterey, CA: Defense Personnel Security Research Center.

Business Transformation Agency. (January 2010). *Defense Business Systems Acquisition Executive (DBSAE)*. (This website is no longer available due to organizational restructuring).

Chandler, C. J. (2002). *ACES pilot program review workshop* (Unpublished manuscript). Monterey, CA: Defense Personnel Security Research Center.

Chandler, C. J. (2008). *Automated Continuing Evaluation System (ACES) overview*. (Unpublished manuscript). Monterey, CA: Defense Personnel Security Research Center.

Chandler, C. J. (2012). *ACES vision for FY12 and beyond*. (Unpublished manuscript). Monterey, CA: Defense Personnel Security Research Center.

Chandler, C. J. (2006). *DHS business rules* (PA 06-09) (FOUO). Monterey, CA: Defense Personnel Security Research Center.

Chandler, C. J., & Jung, C. L. (2007). *Evaluation of ACES business rules for identifying counterintelligence issues* (MR-07-08) (FOUO). Monterey, CA: Defense Personnel Security Research Center.

Chandler, C. J., & Rome, A. P. (2005). *ACES beta test evaluation* (Tech. Rep. 05-14) (FOUO). Monterey, CA: Defense Personnel Security Research Center.

Chandler, C. J., & Timm, H. W. (2002). *ACES program management plan and concept of operations* (MR-02-01) (FOUO). Monterey, CA: Defense Personnel Security Research Center.

Chandler, C. J., & Timm, H. W. (2009). *PERSEREC ACES- and other CI-related projects*. (Unpublished manuscript). Monterey, CA: Defense Personnel Security Research Center.

Chandler, C. J., Timm, H. W., Massey, K. R., & Zimmerman, R. A. (2001). *Defense Personnel Security Research Center database matching pilot study*. (Tech. Rep. 01-01) (FOUO). Monterey, CA: Defense Personnel Security Research Center.

Chandler, C. J., Timm, H. W., Massey, K. R., & Zimmerman, R. A. (2000). DRAFT. *Security Research Center database matching pilot study*. (Tech. Rep. SRC-TR-

00-01) (FOUO). Monterey, CA: Defense Personnel Security Research Center.[15]

Commercial databases containing information relevant to personnel security investigations and research. (1991). (Unnumbered Tech. Rep.). Monterey, CA: Defense Personnel Security Research Center.

Development of a prototype automated continuous evaluation system—ACES. (1999). (Unpublished report). Monterey, CA: Defense Personnel Security Research Center.

DISS status update. (2012). (Unpublished manuscript). Washington, DC: Defense Information System for Security.

DISS update for CAF consolidation meeting. (2012). (Unpublished manuscript). Washington, DC: Defense Information System for Security.

Early, P. (1988). *Family of spies: Inside the John Walker spy ring*. New York: Bantam Books.

Executive Order 12968, *Access to classified information*, August 2, 1995 (as amended by Executive Order 13388, *Further strengthening the sharing of classified information to protect Americans*, October 25, 2005).

Executive Order 13467. *Reforming processes related to suitability for government employment, fitness for contractor employees, and eligibility for access to classified national security information*, June 30, 2008.

Government Accountability Office. (2005). *DOD personnel clearances: Some progress has been made but hurdles remain to overcome the challenges that led to GAO's High-Risk designation*. (GAO-05-842T). Washington, DC: Government Printing Office.

Government Accountability Office. (2012).*Personnel security clearances: Continuing leadership and attention can enhance momentum gained form reform effort*. (GAO-12-815T). Washington, DC: Government Printing Office.

Hadley, S. J. (2005). Memorandum for William Leonard, Director, Information Security Oversight Office from the Assistant to the President for National Security Affairs. Attachment. Revised adjudicative guidelines for determining eligibility for access to classified information. [Memorandum].

[15] From 1997 until early 2000, PERSEREC was renamed the Security Research Center and operated as a part of DSS. In late 1999, between the draft report being submitted and the final report being published in 2001, PERSEREC regained its independence from DSS and took its original name as the Defense Personnel Security Research Center (PERSEREC). In 2013, PERSEREC was aligned under DMDC as the Defense Personnel and Security Research Center.

Helton-Fauth, W. B., Ainslie, F. M., Chandler, C. J. (2013). *Department of Defense/Automated Continuing Evaluation System continuous evaluation: Pilot study results*. (Tech. Rep. 13-03) (FOUO). Monterey, CA: Defense Personnel Security Research Center.

Herbig, K. L. (2008). *Changes in espionage by American citizens, 1947-2007*. (Tech. Rep. 08-05). Monterey, CA: Defense Personnel Security Research Center.

Herbig, K. L., & Wiskoff, M. F. (2002). *Espionage against the United States by American citizens, 1947-2001*. (Tech. Rep. 02-05). Monterey, CA: Defense Personnel Security Research Center.

Heuer, Jr., R. J., Crawford, K. S., Kramer, L. A., & Hagen, R. R. (2001). *A new approach to the SSBI-PR: An assessment of a phased reinvestigation*. (Tech. Rep. 01-06) (FOUO). Monterey, CA: Defense Personnel Security Research Center.

Information Security Oversight Office. (2004, December 14). *Modification to Investigative Standards for Single-Scope Background Investigation—Periodic Reinvestigations (SSBI-PR)*. Washington, DC: Author.

Internal Revenue Service. (nd). Manual. Retrieved June 7, 2012 from http://www.irs.gov/irm/part9/irm_09-005-005.html.

Joint Security & Suitability Reform Team. (2008a). *Security and suitability process reform*. Washington, DC: Office of Management and Budget.

Joint Security & Suitability Reform Team. (2008b). *Draft investigative standards*. (Unpublished manuscript). Monterey, CA: Defense Personnel Security Research Center.

Joint Security & Suitability Reform Team. (2010). *Security and suitability process reform strategic framework*. Washington, DC: Office of Management and Budget.

Kramer, L. A., Crawford, K. S., Heuer, Jr., R. J., & Hagen, R. R. (2001). *SSBI-PR source yield: An examination of sources contacted during the SSBI-PR*. (Tech. Rep. 01-05). Monterey, CA: Defense Personnel Security Research Center.

Memorandum of agreement concerning the transfer of certain elements of the US Department of Defense to the US Office of Personnel Management. (2004). Washington, DC: Department of Defense.

New DoD personnel security program. (1995). (Unpublished report). Monterey, CA: Defense Personnel Security Research Center.

Office of Personnel Management. *Continuous efforts to align with reciprocity goals and timeliness standards*. Federal Investigations Notice No. 11-04, August 29, 2011. Washington, DC: Government Printing Office.

REFERENCES

Richmond, D. A., Chandler, C. J., & Jung, C. L. (2008). *ACES pilot test evaluation for the Department of Homeland Security*. (Tech. Rep. 08-06) (FOUO). Monterey, CA: Defense Personnel Security Research Center.

Rome, Jr., A. P., & Chandler, C. J. (2005). *Automation of the NLETS interface*. (MR-06-03) (FOUO). Monterey, CA: Defense Personnel Security Research Center.

Timm, H. W. (1990). *Improving the efficiency of the Defense Investigative Service credit report acquisition process*. (Tech. Rep. 90-05). Monterey, CA: Defense Personnel Security Research Center.

Timm, H. W. (1997). *Program area: Financial & credit*. (Unpublished report). Monterey, CA: Defense Personnel Security Research Center.

Timm, H. W. (2001). *Estimated impact of the proposed Automated Continuing Evaluation System (ACES) on personnel security effectiveness: A preliminary assessment*. (Tech. Rep. 01-03). Monterey, CA: Defense Personnel Security Research Center.

Timm, H. W., Buck, K. R., & Chandler, C. J. (2004). *Information discovered during automated continuing evaluation system database checks of interest to counterintelligence units.* (MR-05-02) (FOUO). Monterey, CA: Defense Personnel Security Research Center.

U.S. Senate Select Committee on Intelligence. (1994). *An assessment of the Aldrich H. Ames espionage case and its implications for U.S. intelligence*. Washington DC: Government Printing Office.

Zimmerman, R. A., & Chandler, C. J. (2010). *Automated continuous evaluation system (ACES) concept of operations DRAFT*. (Unpublished manuscript). Monterey, CA: Defense Personnel and Security Research Center.

APPENDIX A:

DESCRIPTIONS OF MAJOR ACES PILOT PROJECTS

Name: Database Matching Pilot Study

Start and End Dates: 1998-early 2000

Participants/Case Sources: DoD DSS

Report: (FOUO) PERSEREC Technical Report TR-01-01, February 2001 (Chandler, et al).

Goals/Results: This study assessed the feasibility and value of acquiring computerized data from 15 different government and private vendor databases that were not routinely checked during federal personnel security investigations. For 11 of the 15 databases, PERSEREC secured authorizations to query the databases and provide the resulting information to DSS for use in 500 actual personnel security investigations. Each of the 365 test cases required a subject interview, and each was assigned to one of three Northern California DSS Field Offices. Data derived from the new sources of information were included in official ROI prepared by the Special Agents (SAs). The SAs also completed a survey for each test case in which they evaluated each type of additional information provided for their respective cases. Statistical matches (i.e., finding out how many people in a sample had records pertaining to them in a database without revealing their identities) were also conducted when permissible. A stratified sample of 18,000 DoD employees with recent background investigations was selected to evaluate how often the databases of interest yielded information about personnel in each the subpopulations that undergo DSS security background investigations. These statistical matches helped to compensate for regional bias associated with using a sample limited to only Northern California cases. They also provided information for the four databases that were not authorized for use with the test cases. Key findings included the following: All of the databases evaluated provided information that at least some of the SAs reported were valuable in certain cases. This study helped to identify the rates of issue detection from various data sources being evaluated, when SAs would like to receive that information, and in what format.

Name: Initial Air Force Pilot Study

Start and End Dates: January 2002 - June 2003

Participants/Case Sources: DoD: Air Force and DIA

Report: (FOUO) PERSEREC Technical Report TR-05-14, November 2005 (Chandler & Rome, 2005)

Note: this pilot study was discussed as background to the following pilot study, the ACES Beta Test.

Goals/Results: PERSEREC conducted ACES checks on 14,120 individuals with Air Force TS or SCI access. This was the first ACES pilot study to use “live” data, and

the first to refer cases of security concern to a CAF using JPAS. The AFCAF and the DIA were the CAFs providing adjudicator follow-up. Since results early in 2002 showed that some Air Force personnel in the study no longer held a clearance, refined business rules and additional data sources were incorporated to help filter out persons who had separated from the military. In July 2002, another batch of 9,700 cases was run using the revised rules. Results showed that ACES identified 9.31% of subjects as cases with new issues under the business rules revised in consultation with adjudicators. More than half of the adjudicators surveyed reported that too many minor issues were included under those rules, so in January 2003, after the pilot study was completed, refinement of the business rules on financial thresholds reduced the number of issue cases ACES identified to roughly 5%. This "alpha" pilot study demonstrated that ACES could identify numerous issues of security concern of interest to adjudicators.

Name: ACES Beta Test

Start and End Dates: August 2004 - February 2005

Participants/Case Sources: DoD

Report: (FOUO) PERSEREC Technical Report TR-05-14, November 2005 (Chandler & Rome)

Goals/Results: ACES was beta tested by adjudicators at seven DoD CAFs in order to evaluate the utility of the reports the ACES system generated. The following elements of the system were evaluated: the criteria used to identify issue cases, report presentation, ease of use, user documentation, software functionality, and workload impacts. The beta version of this system used 28 different government and commercial records to identify issues of interest to adjudicators. ACES automatically applied business rules to these data to detect individuals who had new issues of potential personnel security concern. From a sample of 12,710 cases ACES business rules identified 3% of the individuals or cases as having new issues of concern. Following the beta test, a focus group of representatives of the CAFs and service components made recommendations to refine further the business rules to eliminate cases that were considered too minor or already known by the CAFs. Findings of this study suggested that ACES improved the CE of cleared personnel by (1) identifying cases of security concern sooner than they were currently being detected and (2) focusing investigative and adjudicative review only on cases where new issues were identified by the system. Key findings included the following: ACES business rules identified 3% of the individuals or cases as having new issues of concern. Adjudicators reported finding new information or issues of interest in 80.6% of the issue cases detected by ACES and said they would like to receive similar cases in the future in 84.5% of the cases. Some form of adjudicative action was taken in 23.4% of the issue cases.

In addition to writing up the results of the ACES Beta Test in a report, during 2005, 2006, and early 2007 research was conducted on various applications and new data sources for ACES. Some of these studies relied on the data collected during earlier pilot studies. In this period, PERSEREC researched automating the ACES interface with NLETS, the characteristics of real property ownership among clearance holders to establish a baseline against which to identify financial anomalies and unexplained affluence, evaluation of ACES business rules for identifying CI issues, and the use of Suspicious Activity and Form 8300 reports from FinCEN for identifying security and CI issues related to possible financial crimes.

Name: DHS Pilot Study

Start and End Dates: March 2007 - March 2008

Participants/Case Sources: DHS (8 components); included DHS initial, PR, and CE investigations

Report: (FOUO) PERSEREC Technical Report TR-08-06, March 2008 (Richmond, Chandler, & Jung)

Goals/Results: This was the first non-DoD pilot evaluation of ACES; it was conducted in coordination with the DHS. The pilot study was conducted with the participation of eight DHS components: DHS Headquarters, the Federal Law Enforcement Training Center, the Transportation Security Administration, U.S. Citizenship and Immigration Services, U.S. Coast Guard, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and U.S. Secret Service. ACES checks were conducted on 12,802 cases provided by the eight components. ACES reports were generated for a subset of these cases and provided to DHS adjudicators. Adjudicators evaluated the cases and completed a web-based questionnaire regarding the nature of issues found by ACES. Surveys were completed for a subset of 1,015 cases.

Survey results were used to determine the extent to which ACES was able to identify issues of concern for DHS adjudicators, how many previously undetected issues ACES revealed, and how often ACES did not identify known issues. Although ACES missed issues in 108 initial or periodic reinvestigations, almost all of these issues would have been identified by combining ACES checks with the other typical investigative sources such as the SF-86, local agency checks, a subject interview, check of the Defense Clearance and Investigations Index (DCII), employment, and immigration records checks. Results showed that ACES had strong potential by identifying actionable cases in initial and periodic reinvestigations and would be an effective tool for monitoring clearance holders between regularly scheduled reinvestigations. Key findings included the following: ACES identified issues of security concern in 10.7% of the 6,407 initial and periodic reinvestigations, and in 4.3% of the 6,395 CE cases. ACES identified 27 cases with one or more issues that

were missed in previous investigations. Although ACES missed issues in 108 initial or periodic reinvestigations, it identified another issue in 72.2% of these cases. For the 30 cases where ACES did not identify an issue, 16 of the issues were identified from the subject interview only; nine from the SF-86, which was not available to ACES for this pilot; and nine were issues that could have been identified with a business rule change. In none of these 30 cases was the subject's eligibility denied or revoked.

Name: ACES Pilot Study for DHS comparing three ARC strategies for SSBIs with traditional SSBIs

Start and End Dates: March 2008 - May 2008

Participants/Case Sources: Army SSBIs

Report: (FOUO) DRAFT Technical Report, 2010

Goals/Results: This pilot study was the second evaluation of ACES for DHS. It addressed the value of ACES checks for identifying issues of personnel security concern. It evaluated the added contribution of commercial electronic data providers to the ACES-based ARC strategy framed in April 2008 by the JRE. ACES-based ARC strategies offered streamlined alternatives to costly and labor-intensive manual investigative leads. The results of three different ARC-oriented strategies were compared with the results of the traditional SSBI investigations. Key findings included the following: ARC-oriented strategies were credited with investigative information from the SSBIs that would be standard to any approach (e.g., SF-86 admissions, criminal record checks). All ARC strategies and the SSBI investigation performed similarly in detection of issues and issue cases, detecting 83% to 89% of issues and 96% to 98% of issue cases. However, this study demonstrated that the incorporation of ACES-based ARC strategies could provide considerable cost savings over the traditional SSBI investigation.

Name: OPM/ACES Pilot, Phase 1 and Phase 2

Start and End Dates: November 2010 - April 2011

Participants/Case Sources: Navy NACLCs and Access National Agency Check with Inquiries (ANACIs)

Report: (FOUO) DRAFT PERSEREC Working Paper, October 2012

Goals/Results: Phase 1 was an analysis of a small convenience sample of 400 Army NACLC and ANACI investigations; results from analyzing this sample informed the second phase. Phase 2 focused on investigations and adjudications done on active duty, civilian, and contract Navy personnel undergoing either a NACLC or an ANACI. These investigation types are commonly used for S level

security clearance eligibility vetting. Investigation requests came from Navy Submitting Offices across the country. The pilot study included 3,250 NACLC and ANACI investigations submitted beginning in November 2010 through March 2011. In addition to successfully completing the investigations for Navy, the pilot study was intended to address certain research goals related to the potential use of ARC in the vetting process. These goals were as follows:

- Compare similar investigative leads produced by ACES and OPM, regardless of methodology, to determine the most suitable ARC option for implementing the revised FIS for Tier 3 (NACLC/ANACI) investigations.
- Analyze unique investigative leads conducted only by ACES to determine the efficiency, overall quality, and value-added of each, for possible inclusion into the ARC option of the revised FIS.
- Assess the efficiency and effectiveness of the ACES flagging strategy, whereby issues flagged by automated sources provide the basis for expanded investigation, in comparison with the current investigative approach. Evaluate the potential for ARC implementation, as proposed in the May 25, 2011 draft FIS, in the reformed vetting process.

The pilot study involved several Government organizations: OPM personnel identified Navy cases for inclusion in the pilot study, conducted the traditional NACLC and ANACI investigative elements, reviewed cases for investigative expansion, generated a ROI for each case, and coded issues identified by OPM and ACES investigative elements.

PERSEREC completed the ACES checks, forwarded the checks to OPM, and provided personnel to assist in the development of the data collection instrument, oversee the quality control processes during coding, conduct the analyses of issues data as coded by OPM coders, and generate the results briefings and final report. Navy adjudicators reviewed and adjudicated cases. The Office of the Director of National Intelligence Special Security Directorate (ODNI-SSD) provided oversight and coordination between agencies and developed the data collection instrument.

Results of this complex study were nuanced. ACES checks proved more timely and less costly for similar issue identification rates in many instances, while OPM traditional checks (which are not directly comparable to ACES checks) identified more issues in other instances. The SF-86 proved the most productive source of issue information. Recommendations focused on how to incorporate ACES checks with the most productive of the traditional investigative checks to enhance the background investigations' effectiveness while minimizing its cost and the time it takes to perform them. Among key findings were the following: The NACLC ARC strategy would have detected 99.7% of the adverse issues, compared to 99.2% detected by the traditional investigation. The NACI ARC strategy detected 99.6% of the adverse issues, about 1 percent more than the traditional ANACI (98.7). Of the 8 cases with issues missed by the ARC strategies, none were adversely adjudicated.

Name: DoD/ODNI ACES Pilot Study

Start and End Dates: May 2011 - March 2012

Participants/Case Sources: Army NACLCs

Report: (FOUO) PERSEREC Working Paper WP-12-02, April 2012

Goals/Results: This pilot study focused on investigations and adjudications of 1,478 Army recruits undergoing a NACLC, an investigation type commonly used for S clearance eligibility vetting. Investigation requests came from 13 Army Recruiting Stations, across the country, operated by USAREC.

In addition to successfully completing the investigations for USAREC, the pilot study was intended to demonstrate that a number of key JRE reform concepts could be achieved, including: (1) Demonstrate an E2E electronic process from initiation of a personnel security or suitability investigation to adjudication, using existing systems, (2) Utilize the eAPP, USAREC's version of the e-QIP, to complete the SF-86, (3) Collect and transmit fingerprints electronically, (4) Evaluate the effectiveness using ACES in the ARC-based investigation and flagging approach.

The pilot study involved several organizations, both government and commercial. Those involved in investigative or adjudicative activities employed existing automated systems or processes that were brought together to create the E2E electronic process (see page 31 for a list of the organizations that participated and their roles). Recommendations included: DoD should consider incorporating ACES-based ARC investigations into the accessions process for entry into military service; DoD should consider the long-term cost-avoidance possible if the process demonstrated in the pilot study were implemented more broadly in DoD; and DoD should consider adopting the Extensible Markup Language (better known as XML)-tagged ROI within 1 year. Among the key findings were the following: Results demonstrated that the overall E2E process using existing capabilities was successful, timeliness goals were achieved (15 days faster than the ISP's current benchmark for traditional investigations), ACES and the SF-86 were the two most productive sources of issue cases, and adjudicator feedback on using the focused ROI was overwhelmingly positive.

Name: DoD CE Pilot Study

Start and End Dates: April 2012 – September 2012

Participants/Case sources: DoD contractor personnel

Report: (FOUO) PERSEREC Technical Report TR-13-03, April 2013 (Helton-Fauth, Ainslie, & Chandler)

PERSEREC conducted this study for the JRE to examine ACES in terms of CE as envisioned in the September 2011 Draft FIS. With the issuance of the final FIS in

December 2012, these specific requirements were deleted. Nevertheless, the findings of this pilot study will help inform the implementation of the revised FIS CE standards. This DoD CE Pilot may also have a collateral impact on the ongoing deliberations regarding improved insider threat guidelines.

The goals of this Pilot were as follows:

(1) Demonstrate the proposed reformed CE process for Top Secret/Sensitive Compartmented Information (TS/SCI) from a random selection of subjects through adjudication.

(2) Assess the value and costs associated with:

  (a) selecting individuals for CE at different 1-year intervals since their last investigation in order to identify the most efficient (higher quality-lower cost) year interval for CE, and

  (b) the ACES checks that produce the most significant, adjudicative-relevant information.

(3) Demonstrate the ability to detect insider threats and security issues through CE and at different year intervals since the last investigation, and earlier than would otherwise be conducted under the PR cycle.

(4) Determine the value-added of the ACES suite of checks for identifying issues of personnel security and/or CI concern.

(5) Obtain adjudicator feedback on the practical utility, perceived quality, and value-added of the ACES checks relative to the current investigative process.

(6) Identify potential changes or enhancements to ACES that would benefit the end-user.

Using JPAS, PERSEREC identified cases eligible for inclusion in the CE Pilot Study, selected a random sample of 2,500 candidates, and stratified them into year intervals representing the number of years since their last investigation (from 1 year to 4.5 years). Because 6 cases were removed from the sample due to loss processing, the final sample for this Pilot consisted of 2,494 contractors cleared for SCI eligibility, with nearly 500 cases in each 1-year, post-adjudication interval. Selected candidates were input into ACES and validated against JPAS via the ACES real-time web service to ensure that each subject maintained their SCI clearance (loss processing) with the participating DoD Agency. Subjects who no longer held a clearance with the agency were dropped from the Pilot Study, and the remainder were subject to the ACES checks. ACES check results were compiled into the ACES subject reports and sent to the Participating Agency, which adjudicated the cases and determined where investigative expansion was required. Data required for analyses were extracted from the ACES database, and collected via survey and a focus group, in accordance with the Research Plan. Among the key findings were

the following: Results indicated that the ACES-based ARC option, when the SF-86, subject interview and local agency checks were included, identified issues at a nearly identical rate (78%) to the SSBI (78.7%). The rates of issue identification for the two electronic data provider ARC options were slightly lower at 75.2% and 69.4%. However, each investigative strategy identified different issue cases. The traditional SSBI missed 35 cases detected by the ACES-based ARC option, while the ACES-based option missed 23 cases detected by the SSBI. The two electronic data provider options missed more of the issue cases identified by the SSBI than did ACES.

Name: Army CE Pilot Study

Start and End Dates: June 2012 – Completed

Participants/Case Sources: Army

Report: (FOUO) DRAFT PERSEREC Technical Report, 2013

Goals/Results: In 2011, PERSEREC, the Department of the Army, Office of the Deputy Chief of Staff, G2 initiated a pilot project to test new technologies and data sources that could help detect or deter insider threats by continuously evaluating the reliability, trustworthiness, and ability to protect classified information of the Army's cleared population. The project randomly selected a sample of 4,000 cleared Army personnel and then used their PII to conduct checks using ACES, social media queries, and a commercial data provider of public records (bankruptcies, liens, judgments, or jail bookings). Concurrent with these checks was exploration of a proof of concept for a risk-rating algorithm by a commercial vendor. The risk algorithm, when fully developed, will incorporate multiple data points to assess the level of risk an individual presents to the organization.

This pilot demonstrated the capability to identify derogatory information about subjects with eligibility for access to classified information before their next PR. Key findings included the following: Approximately 22% of the cases had security flags; Special Investigations (SPINs) were conducted on roughly 5% of cases. As of May 16, 2013, there were 35 revocations and 18 individuals given conditional access. ACES identified significant issues of concern that had not been reported, including 24 individuals with unpaid debt in excess of $25,000. In 13% of issue cases, ACES identified issues in two or more adjudicative categories.

Name: DoD Small Army CE Pilot Study

Start and End Dates: August 2012

Participants/Case Sources: Army

Goals/Results: The objective of this pilot study was to determine the utility of ACES checks in the conduct of internal investigations. Army reported that the results were useful. No further information regarding results is available due to the sensitive nature of the evaluation.

Name: Department of State (DoS) Pilot Study

Start and End Dates: April 2013 – in progress

Participants/Case Sources: DoS

Goals/Results: Pilot study is in progress.

The primary objective of the pilot is to assess the value of individual ACES records checks as an enhancement to the DoS investigation or to replace some of the current DoS investigative leads. The pilot will be accomplished by conducting ACES records checks on a sample of about 1,000 closed initial SSBI. The pilot will also assess a number of key variables associated with the Security and Suitability process reform, to include the cost of the ACES checks, the time elapsed to complete them, and the investigative productivity of the ACES checks.

Name: Army Accessions Pilot Study

Start and End Dates: Planned for summer 2013

Participants/Case Sources: United States Military Entrance Processing Command (USMEPCOM) and USAREC

Goals/Results: Pilot study is in progress.

The primary goal of the pilot study will be to examine ARCs, including ACES data sources, as they pertain to the requirements for identifying applicants who may be disqualified from military enlistment in the earliest stages of the recruitment process. The objectives are to provide earlier detection of disqualifying factors and to demonstrate that earlier detection results in reduced program and training costs.

A secondary goal of the research will be to address medical pre-screening conducted by the Military Services through evaluation of Electronic Health Records (EHR) existence, accessibility, and automated capability. The objectives are to identify EHR systems or Health Information Exchanges that provide a method for sharing EHR among disparate care providers; to identify and compare EHR providers regarding their services, coverage, anticipated costs, and enrollment requirements; and to determine the extent to which existing EHR can be integrated into the medical screening process and subsequent DoD health information systems.