Interested in learning more about security?

SANS Institute InfoSec Reading Room

Leveraging the Federal Public Trust Clearance Model in State Government Personnel Security Programs

Security clearances are a requirement when working with classified information at the federal level. In recent years, incidents involving unauthorized disclosures of highly sensitive classified information have brought the security clearance adjudication process under scrutiny. These incidents have reinforced the principle that a personnel security program that properly vets individuals is critical to any organization that wishes to protect its data. Although the effects of an incident at the state level may be narrowe...

Leveraging the Federal Public Trust Clearance Model in State Government Personnel Security Programs

GIAC GSEC Gold Certification

Joseph C. Impinna, joseph.impinna@ftb.ca.gov
Advisor: Stephen Northcutt
06/18/2015

Abstract

Security clearances are a requirement when working with classified information at the federal level. In recent years, incidents involving unauthorized disclosures of highly sensitive classified information have brought the security clearance adjudication process under scrutiny. These incidents have reinforced the principle that a personnel security program that properly vets individuals is critical to any organization that wishes to protect its data. Although the effects of an incident at the state level may be narrower in scope than at the federal level, the need to safeguard sensitive information is the same. The national security clearance model is used at many state agencies that work with the Department of Defense and other federal entities. However, an agency that does not access national security data still has a responsibility to uphold public trust. For these organizations, the background check processes can vary greatly from state to state or even between agencies.

An effective personnel security program is much more than simply granting access to protected information through a public trust clearance. To achieve the assurance implied with a clearance, other components must be included. While a direct implementation of the federal model may not be feasible, using just a few concepts to design a system tailored to the state level would significantly improve the security posture of the issuing agency.

1 Introduction

On August 28, 2014, one of the most prolific spies in the history of U.S. espionage passed away quietly in a North Carolina federal prison. For 18 years, U.S. Navy Warrant Officer John A. Walker worked as a double agent for the Soviet Union (Earley, 1988). Nearly 30 years after his arrest, several books, and a TV movie, the impact of one man's treason is still difficult to comprehend. Due to his privileged position as a communications officer with a Top Secret national security clearance, Walker had access to privileged information on a wide range of topics covering NSA cryptologic keys, ship's movements, detailed nuclear submarine specifications, and naval strategy that led to "dramatic Soviet gains in all areas of naval warfare" (Gordon, 1987). The breadth and depth of the secrets Walker sold for less than $1 million almost single-handedly destroyed the U.S. nuclear advantage at the height of the Cold War. Despite Secretary of the Navy Caspar Weinberger calling for a more draconian punishment, he was sentenced to a single life sentence with the possibility of parole (Sontag & Drew, p. 273); the friends and family members he recruited were also convicted. The Walker name has become synonymous with treason and breached trust to those in Naval intelligence and communications circles (significant enough to be included in Navy training curriculums). The crimes he perpetrated less than 50 years ago are now largely a footnote in history. However, the methods and motivations are no less prevalent, and these incidents continue with the likes of Snowden, Manning, and other lesser known names illegally removing and exposing the data that had been entrusted to them. Whether one refers to these incidents as acts of courage against an overreaching government or espionage against their nation, the simple fact remains that it is a threat to the employer and the deeply interconnected global IT environment assists in facilitating these crimes.

The defense in depth strategy is designed to take a holistic approach with security programs at every level of the Open System Interconnection model (OSI). Personnel security is a precursor to architecting an IT environment. Technical controls cannot provide adequate protection for systems and data without administrative controls such as a personnel security program that identifies qualified and trustworthy employees. Once a program is implemented, enforcement mechanisms (including classifying and identifying ownership of data, systems, and

Impinna, joseph.impinna@ftb.ca.gov

job positions) become the foundation on which controls are built. Humans are often the weakest link in any robust information security program, and a small gap is all it takes to peel away multiple layers of an organization's security posture. In 2014, the Department of Defense (DoD) revoked 4,136 security clearances from individuals found to exhibit high-risk behavior (GAO, September 2014). As security researcher Eric Cole puts it, the human is the "operating system that is hard to control and impossible to patch" (Cole, 2014).

Some of the world's largest corporations and government agencies, at all levels, have fallen victim to the insider threat, proving that it is not limited to any particular sector or vertical market. Whether military or civilian; private or civil service employees; or motivated by greed or feelings of antipathy, the common thread is that they were all trusted employees who had been previously granted security clearances before breaking the trust granted to them by their employer. While these and other breaches are well-publicized, the federal government has a fairly mature and reliable process for screening out high-risk candidates. But, what about personnel security practices at other levels of government? The requirement to identify these positions may come from legislation; but if absent, it is left up to agency policy.

For organizations wishing to implement such a program, the answer is to issue a public trust clearance that includes procedures for conducting background checks for employees, the scope of which is tied to the job position. However, for a clearance to have any impact, there are three key components that must be included:

1. Positions of public trust must be designated.
2. Information must to be properly classified.
3. The network architecture must provide the security controls necessary to enforce these restrictions.

Public servants have a duty to ensure that the taxpayers are getting value for their money. This is codified at the federal level (Code of Federal Regulations, 2012), and many states and municipalities have legislation to identify public trust positions and screen personnel filling those positions. This control is also required in industry standards, such as National Institute of

Standards and Technology Special Publication (NIST SP) 800-53, but a more important concept comes into play. Civic duty and personal integrity must be personally held beliefs, especially for those that serve in leadership or decision making positions. Civic leaders owe it to the taxpayers to say that only the most highly qualified and responsible people are being placed in public trust positions.

1.1 Scope

This paper will examine why implementing a comprehensive personnel security program is a significant challenge at the state level. Through my dual careers, I have experienced this issue from opposing perspectives. As a security analyst working in state government, I understand the risk involved with granting access to trusted insiders that have not undergone extensive background checks; as a Naval Officer, I know that the seemingly limitless resources of the federal government makes providing these controls a much easier proposition.

Our complex federal bureaucracy makes much of the security clearance model outdated, cumbersome, and unnecessary. The process was designed in the 1950's (Joyner, 2013), but the world has changed immensely in the past 60+ years. While there are well documented gaps in the system, suggesting improvements to the federal security clearance process is an entire paper in itself. Nor is this a referendum on the activities that clearance holders are engaged in. Despite any beliefs the reader may hold to be self-evident regarding liberty and privacy from the federal government, the reality is that from a data security perspective, all organizations have information to protect. Thus, the need for some measure of personnel security is the same whether it is the National Security Agency (NSA), a large international corporation, or a small "mom-and-pop" business. This paper will propose a guide for state agencies looking to leverage the framework used by the Office of Personnel Management (OPM) while adopting their own procedures. Additionally, federal law will be referenced, but this is applicable only to agencies within the executive branch. State agencies must assess existing legislation to determine if the framework suggested here is feasible for their climate. The selection of controls, both administrative and technical will be based upon the risk management framework described in NIST SP 800-39.

This paper will also be limited to discussing personnel security for state agencies that do not access national security or law enforcement data. These agencies follow established processes to request national security clearances as a pre-requisite for data exchange.

Finally, this paper is not meant to be a case study on any particular incident, but the Walker, Snowden, and Manning cases all exhibited similar breakdowns in personnel security that contributed to the breach. These failures are too numerous to overlook and demonstrate how important a comprehensive background check and transparency are to the entire process. Ultimately, they serve as examples of what not to do with a personnel security program.

2 Background

Executive Order (EO) 10450, signed in 1952 by President Eisenhower, was the first act to codify personnel security requirements throughout the executive branch. By "establishing and maintaining within his department or agency an effective program to insure that the employment and retention in employment of any civilian officer or employee within the department or agency is clearly consistent with the interests of the national security", the president aimed to both prevent malicious users from accessing sensitive information and identify suspected traitors. Previously, personnel security was a patchwork affair, with enforcement coming through legislation that was limited in scope and agency policies that differed throughout the executive branch.

Although information at that time was mostly in paper format, there was a primitive form of data security: controlling physical access to restricted information. Executives had great discretion in deciding how and to whom security clearances would be granted. Now, in the age of data security, risk management practices and data classification standards must be consistently applied throughout the government. In 2008, EO 13467 reformed the processes to keep-up with technology by determining the eligibility for "logical and physical access"; requiring that investigations and adjudications employ "end-to-end automation to the extent practicable"; and perhaps the most significant gain, requiring continuous evaluation "at any time during the period of eligibility". This order also required an aligned system to conduct investigations and reciprocally accept favorable clearance determinations across all agencies of the executive

branch. While it is always a challenge for an organization to break away from the "stovepipe" business model, ultimately a baseline set of standards that can be applied uniformly is a big win for anyone for whom the government is in possession of personal information. Which, as the NSA domestic monitoring program has revealed, is pretty much everyone.

2.1 Understanding risk factors

Another way to think of personnel security is of performing risk assessments against humans. In this way, it is no different than any other component of a comprehensive information security program. As human nature is dynamic, complex, and often unpredictable, assessing this risk can be a terribly difficult proposition. Adjudicative guidelines can differ based on the agency, but the table below lists the factors to be considered in federal investigations (DNI, 2008). These are not weighted, but used to develop a "whole-person" concept.

Allegiance to the United States	Foreign influence	Foreign preference
Sexual behavior	Personal conduct	Financial considerations
Alcohol consumption	Drug involvement	Psychological conditions
Criminal conduct	Handling protected information	Outside activities
Use of information technology systems		

Table 1, Risk factors to be considered during adjudication

Source: Intelligence Community Policy Guidance 704.2

Adjudicating a clearance is a multi-step process that attempts to piece together a complete picture of a candidate's life with the goal of determining if granting access would present undue risk to the organization. Only after all these factors have been considered can a decision be made as to whether to adjudicate a clearance. The Walker case provides a textbook example of the financial risk factors he exhibited making him an easy mark for a payoff. A credit check alone would have revealed the second mortgage he took out to open a bar; a questionnaire and personal interview would have revealed that he was staying in Norfolk during the week and making a 400-mile round trip on the weekends to visit his wife and four kids in Charleston, SC. His

$120/week check was barely enough to support two households, so he was borrowing heavily from family and friends in a sort of pyramid scheme to pay off debt and keep the bar afloat (Earley, p. 56). Had this information been discovered, his clearance suitability most certainly would have been suspended pending investigation, if not revoked altogether.

2.2 Types of clearances

The federal government defines two positions that require background checks: public trust positions and national security positions. As one would expect, the clearance process one must undergo before being declared eligible for a national security position is far more rigorous than a public trust position. As mentioned earlier, this paper will only examine the public trust position process, as it is sufficient to vet individuals that are candidates for public trust positions in civil service that do not have national security implications.

2.3 Efficacy

To justify the expense of conducting background investigations for those in leadership positions, to, they must ask the question: does a clearance really matter? Although the aforementioned GAO report identified areas for improvement in the security clearance process, revoking a clearance is a fairly rare occurrence. Indeed, as a percentage, the number of revoked DoD security clearances is extremely low, with less than 0.1% of cleared individuals losing their access in 2013. One would expect, considering the volume of cleared personnel (and the amount of data under DoD control), that more reportable incidents would occur. The background check looks for flags, such as financial problems and foreign allegiance, which raises the risk of individuals who would compromise information in exchange for a payment. Catching these issues up front ensures that high-risk individuals are never granted a clearance, and most revocations are due to issues that took place after the background check was completed. It should be noted that the GAO report also identified concerns about the DoD's methodology and record keeping, so this data likely does not include all cases.

You do not need to be well versed in the intricacies of the clearance process to understand this concept; anyone with the most basic understanding of human nature knows that predicting a person's behavior begins with examining their past.

2.4 Catching what slips through the cracks

A Single Scope Background Investigation (SSBI) is required for the highest level clearances, and it thoroughly investigates ten years of a candidate's history. However, some agencies require a final safeguard for contingency of employment: the polygraph. Polygraphs are a controversial topic and opinions run the gamut. Those who have taken one would admit it is unnerving and intrusive. Others say it is a critical tool, and still others would even call it junk science. For the author, who has completed a poly exam, the truth lies somewhere in the middle. Regardless of the veracity of the results, the true value of the polygraph lies in the fact that it gets people to admit to details that were either omitted or lied about during the earlier stages of the clearance process. Regardless of opinion, a polygraph examination is required if one wishes to fill a position that has access to the highest data classifications.

Remember then, that everything is about the risk. Are state agencies handling information that is so sensitive they need the assurance of a polygraph exam? For example, some agencies require employees to pass a polygraph exam before granting access to Top Secret/Sensitive Compartmentalized Information (TS/SCI), which is defined as information that could be expected to cause exceptionally grave damage to national security (Exec. Order No. 12356, 1982). If so, the agency should be using a federal information system and clearance issued by OPM or DoD. Thus, passing a polygraph is an unnecessary step that adds expense without reducing risk, which is why it is omitted from public trust clearances.

2.5 Legal implications

It is a commonly accepted legal fact that an employer can be held legally responsible for the bad actions of an employee. For example, if a bank knowingly hires someone with a criminal history in white collar crime, and that employee embezzles funds from customers, the bank can be held responsible for their negligent hiring practices. This also applies to government agencies and employees. With that in mind, hiring processes that ensure that positions are being filled by qualified and suitable individuals can mitigate this risk.

There may also be legal roadblocks to implementing such a system. Although it is unlikely civil service laws would prohibit any type of background check, some states may require new legislation to give any proposal traction and the political will to proceed.

Impinna, joseph.impinna@ftb.ca.gov

2.6 Privacy Issues

Perhaps the most challenging legal and ethical issue related to background checks is a candidate's privacy. Most states have privacy legislation that defines standards on collecting personal data. Beyond the legal restrictions, the government has an ethical duty to collect and maintain the data of private citizens no more than is necessary to perform legal government functions, with public safety and tax collection being prime examples. Every security control needs an audit mechanism, and a personnel security program is no different. There must be safeguards in place to ensure that the information collected during the background check process is not maintained longer than necessary, nor recycled for use in other activities.

The most powerful revelation from the Snowden case was not necessarily the volume of data that the NSA was accumulating, but the numbers on how many people were impacted. The NSA tapped into the links between Google private cloud servers, allowing the agency to "collect at will from hundreds of millions of user accounts" (Gellman & Soltani, 2013) While this is an emotional topic for many, it is important to distinguish between domestic surveillance activities and a background check being conducted with expressed consent. Applying the standards in the Fair Credit Reporting Act to the process will help ensure that an employer stays within their rights. Ensuring that the information gathered is relevant to the job and gaining consent are the two ways an employer can protect themselves (FCRA, 1970). Although civil service laws may differ from state to state, one factor that is similar to the private sector is a key component of the hiring process: contingency employment. The typical requirement for civil service is that any conditions for employment must be defined for applicants. The following steps ensure that candidate privacy is respected and provides transparency to the process:

1. Adjudication guidelines must be defined.
2. Background investigations must be conducted by a party separate from the hiring process.
3. Flags discovered during the process are reported, but other information discovered that does not factor into a person's risk level should not be taken into consideration.

4. A group or committee reviews the flags and makes a determination on whether to proceed with hiring, ask the candidate follow up questions, or reject outright.

5. Any information gathered during an investigation should be expunged upon completion of the investigation.

2.7 Cost-benefit Analysis

Often times, agency executives must be educated on current threats before they are willing to commit resources to the security program. CSOs must drill in a core principle of information security: one must assume that insider threats are always present. This can be a touchy topic, as it may give the perception that employees are not to be trusted. During a tense moment before signing the Intermediate-Range Nuclear Forces Treaty, President Reagan famously quoted the Russian proverb of "Doveryai, no proveryai" – trust, but verify[1]. Essentially, he was saying that the Soviets and Americans needed to keep each other honest. Once executives understand this concept, the next step of the decision making process is performing a cost-benefit analysis to determine if it is worth the expenditure of taxpayer funds. Like so many other security programs, success is often measured as cost avoidance rather than monetary gains. The cost of incident response is often calculated using historical values and estimations. It would seem that program costs are more straightforward, but in reality both values are difficult to quantify.

2.7.1 Costs

OPM conducts all investigations for federal public trust clearances. A recent notice listed costs of between $210 and $3,959 per investigation (OPM, 2014). Estimating the cost for the entire process varies greatly depending on the type of clearance, additional coverage, and other variables. A Single Scope Background Investigation (SSBI) is far more expensive than a National Agency Check with Law and Credit (NACLC). While state agencies would not be procuring OPM services, these numbers provide a reference point for investigation costs.

A major benefit of implementing a unified public trust system is reciprocity. Agencies in the executive branch are required to use this system and may not implement their own clearance processes (Code of Federal Regulations, 2012). Applicants can leverage an existing clearance

[1] In one of history's great ironies, this quote was made famous by Vladimir Ilyich Lenin.

from a current or former employer to apply for another. This has many benefits, including saving the new employer the expense of conducting a background check for someone whose clearance has already been adjudicated. This also helps widen the talent pool that agencies can draw from.

2.7.2 Cost avoidance

The costs to clean up even the smallest breach can reach into the millions of dollars, and that only includes the direct impacts. The NSA estimates that the incident response alone for the Snowden breach has reached into the tens of millions (Ledgett, 2013). Expand the scope of the estimate to include the loss of public trust that reaches into the private sector and the number is mind-boggling. A recent Forrester report noted that the fallout will cost cloud and outsourcing providers about $47 billion in revenue over the next three years (Dignan, 2015). Certainly, the Snowden affair is by far the most expensive data breach in history and far outside the statistical average. That then begs the question: what is a "normal" breach? As there are so many unknowns, it makes the decision a bit easier: if the agency handles any type of sensitive data, implementing a personnel security program is a wise investment of funds.

3 Recommendations

How then does a state agency with limited resources provide the assurance that employees are being properly vetted before being placed in public trust positions? The term "background check" is vague and, depending on the criteria, may be as simple as a reference check or as thorough to include a polygraph exam. When assigning risk to positions, agencies must determine how rigorous a background check is required to provide assurance. Many factors must be considered when building the background check requirement. For most agencies, public trust clearance provides adequate assurance for sensitive but non-national security information. Appendix 1 includes a listing of the types of clearances used at the federal level, and how similar investigative processes can be applied to a state agency.

OPM investigative services are only available to non-federal agencies that have a need for access to federal information. Thus, states should use the federal system as a model, and then design a program based on their own requirements.

Impinna, joseph.impinna@ftb.ca.gov

3.1 Clearance granting process

The lifecycle includes two main activities: investigation and adjudication. A third activity, continuous monitoring, addresses the gap between investigative periods. It is important to discuss how two stakeholders share responsibility in the process, which provides a strong separation of duties. The agency must first define public trust positions that require a clearance, and OPM then conduct an investigation based on the standards outlined in the Code of Federal Regulations section 731.106. The requesting agency's head is responsible for reviewing findings and making a determination on suitability. Thus, OPM serves as a neutral, third-party that is separate from the employer and job candidate. In the past, background investigations were outsourced to private contractors. However, this practice has been reformed. Since 2007, at least 18 investigators have been convicted of falsifying investigations (Hosenball, 2013). The revelation that red flags were missed during Edward Snowden's background investigation (Grand, 2013) was the straw the broke the camel's back. Congressional hearings have led to reforms, starting with OPM now insourcing the quality review for investigations (Kyzer, 2014).

3.1.1 Investigation

An investigation is initiated with a candidate filling out a form after being offered a position. To give the applicant assurance that this step remains separate from the rest of the hiring process, it is important to gain permission to proceed with a background investigation only after a contingent offer has been accepted. After the requestor submits the completed form, an investigation commences. The extent of the information requested on the form, and the ensuing investigation is linked to the clearance level, which is in turn dictated by the risk level of the position.

Designing a new program offers the opportunity to close gaps in the OPM's investigative standards. For example, a low-risk clearance investigation does not include a check of local law enforcement agencies. Including this check in all investigations might give the clearance a bit more assurance for state and local agencies. While these standards have been updated in recent years, social media checks are also missing. In 2015, a background investigation simply cannot be regarded as exhaustive unless, at least, a minimal check of social media is included, such as conducting a check against freely available information such as a publicly accessible Facebook

site. Any information gathered should be used to add context to an investigation, and not as the sole adjudicating factor. A recent GIAC Gold Certification paper (Hubert, 2014), detailing a comprehensive methodology of how to collect and preserve social media evidence, is a good start for an agency looking to incorporate this information into background investigations. While Hubert's case study details how to conduct a social media investigation into a current employee, the methods can be used for pre-employment checks as well.

Legislation is evolving and has not yet completely caught up with this technology. Laws vary from state to state, but currently 23 states have legislation under consideration regarding employer access to social media (NCSL, 2015). Including social media research in background checks should involve unauthenticated access. Accessing protected social media, such as requiring a candidate to share their username and password to private content, should never take place without a thorough understanding of the legalities.

Descriptions of investigative criterion used by the OPM are contained in appendix B.

3.1.2 Adjudication

After the investigation concludes, the application proceeds to the next phase of the process. Adjudication is an analysis of the information gathered during the investigation and making a determination on the suitability of a candidate. Essentially, this is conducting a risk assessment on humans.

Security risks are not the only reason an agency might consider a security clearance program. The hiring process can be lengthy and frustrating for government positions, and one contention is that the civil service system does not grant managers the same leeway as those in the private sector to tailor their workforce to meet business requirements. Adjudication should also include a second level of review to ensure objectivity before someone is hired to protect both the hiring manager and the agency from any possible accusations of unfair hiring practices. It can also ensure that the hiring process remains above board by ensuring that other issues, such as discrimination or nepotism, do not factor into employment decisions.

3.1.3 Continuous monitoring

It is not enough to conduct an initial pre-employment background check. Periodic reinvestigations must be conducted to ensure that risk factors are identified as soon as possible, rather than at the next scheduled interval. While federal law requires agencies to conduct background checks at accession, it also requires agencies to upgrade the investigation within 14 days of a change to a higher position risk level (Code of Federal Regulations, 2012). NIST also requires personnel screening (and re-screening) as a baseline security control for all information system risk classifications (NIST, 2014). The substance of reinvestigations may be determined by the agency, but the intuitive answer would be that the type of investigation conducted is proportional to the risk level of the position.

The Snowden incident can be directly tied to the lack of continuous monitoring. After his activities became public, quick online searches revealed that he had been an active contributor to the technology site, Ars Technica, since 2001, including commenting on topics such as masking internet activity and disdain for government wiretapping (Mullin, 2013)[2]. This reveals two conspicuously missing gaps from the federal clearance process: the fixed length of time between re-investigations and the lack of social media research in the investigative process. If either of these controls had been included, they may have revealed flags. While making comments on an internet message board may not be sufficient in itself to disqualify one for a clearance, it certainly would be identified as a possible risk factor, which in turn may have led to a re-investigation to determine clearance suitability. Continuous monitoring is listed as number 4 in the SANS Top 20 critical controls. A gap between background checks is a gap in the personnel security program.

3.2 Using controls to enforce a clearance

Organizations can implement the most robust personnel security program, with unlimited resources allocated to pre and post-employment checks to validate employees. However, this

[2] The reader comments on this article reveal a fascinating dichotomy about the mixed emotions and confusion over the Snowden incident, and the concept of online privacy. While Ars Technica includes a disclaimer during user registration, readers ironically found the analysis of public content "creepy". One reader stated "Isn't the ability to go searching through a person's entire internet history kinda what he is fighting against? I mean, we all realize that stuff is out there forever, but I agree...creepy." (Mullin, 2013)

would not be the foundation for an effective information security program. Rather, the two are complementary. Technical controls must be employed to provide the assurance that the clearance program is effective; the personnel security controls ensure that technology and data are being managed by the right people. Three critical components must be implemented to protect the integrity of the clearance.

3.2.1 Designating positions of public trust

Assumption: Positions of public trust have been identified throughout the organization. Individuals in these positions will be granted a higher level of privilege and access based on an adjudicated clearance and a need to know.

Perhaps the most critical element of a personnel security program at a public agency is identifying public trust positions. Even if not required through legislation, it is best practice and a NIST recommended control. Roles might include positions of decision making power, fiduciary responsibility, and access to operational controls.

The need-to-know concept is an important mitigating factor to providing security clearance. When one is granted a clearance, they are said to be eligible. This is important, because it indicates that the individual *may be* granted access to the specified classification level. Access is actually granted to the position (i.e. analyst, system administrator, etc.) that the individual fills. Figure 1 details this process.

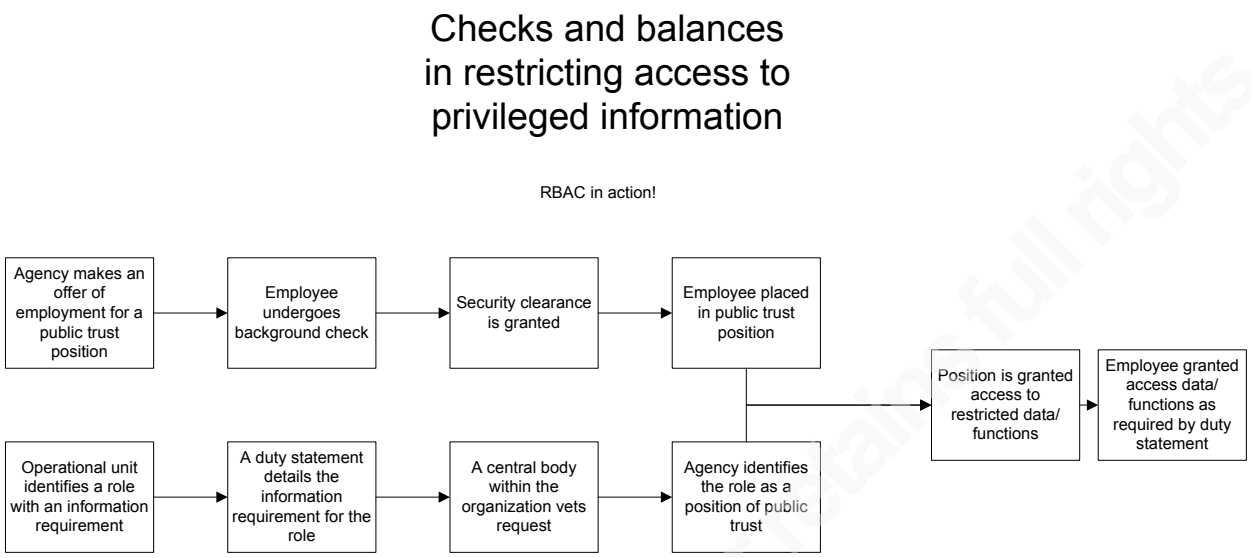

Figure 1, Checks and balances in restricting access to privileged information

Civil service employment includes both a job classification (pay grade) and duty statement. For example, while a project manager and a server administrator may be in the same pay grade, their duty statements (and level of responsibility) are vastly different. Organizations should ensure that public trust positions are designated by duty statement, and not job classification.

This is not a groundbreaking proposal: it is essentially how the Role Based Access Control (RBAC) model is implemented. Roles must be defined at the enterprise level through an official channel, such as an action committee with representation from multiple business areas to maintain integrity. For a large organization, this can be a daunting task. Fortunately, OPM provides a free Position Designation tool to assist with this process.

3.2.2 Classifying data

Assumption: Information and systems are properly classified. The classification level of the data contained within does not exceed that of the system or application.

The ultimate goal of every security control is to protect data. As it has been said in many different ways, "you cannot protect what you cannot identify." A robust data classification program must be employed that includes all information assets used by the organization. Federal Information Processing Standards Publication (FIPS) 199 contains standards for categorizing

information and information systems. These are examples of complementary controls. The two are differentiated, and indeed, one cannot have one without the other. One example of this is the often maligned Microsoft SharePoint Content Management System (CMS). It is easy to blame SharePoint's distributed security model as an easy attack vector for data exfiltration and indeed the Manning incident was perpetrated by retrieving data from a SharePoint site (Zetter, 2011). A recent study discovered that a paltry 9% of organizations are marking their documents (Infosecurity Magazine, 2013). No wonder then, that it can be so easy to remove sensitive data from SharePoint. Without both a strong governance model and data classification, a powerful business tool can become a liability.

3.2.3 Other technical and administrative controls

Assumption: The network architecture provides the security controls necessary to protect the data.

After data has been classified and located appropriately, the next step is employing access controls to grant access to authorized individuals, and restrict access from unauthorized individuals. This is a circular reference of sorts, but an important point to make nonetheless as this is how a federal security clearance is enforced. A brief examination of DoD network architecture illustrates how true physical separation of networks at layer one of the OSI model is implemented, to the extent possible. The Nonsecure Internet Routing Protocol (NIPRNET), Secure Internet Routing Protocol (SIPRNET), and Joint Worldwide Intelligence Collection System (JWICS) all use dedicated infrastructures. Connections to the Global Information Grid (GIG) are provided via a core backbone router. Where necessary, SIPRNET connections are routed over NIPRNET or the Internet via an encrypted tunnel. While it is nearly impossible to create a true physical separation of WAN links, this architecture provides separation of networks of different classifications at layer one of the OSI model at the LAN level. In fact, to mitigate the risk of network bridging, different cabling media is required where networks are co-located. The resources required to maintain multiple physical networks explain why this architecture is rarely employed at locations that do not have a national security mission or other regulatory requirements that require physical separation such as SCADA or ICS networks.

While controls are automated to the fullest extent possible, humans must enforce the policies. The federal government employs a Special Security Officer (SSO) to enforce access controls, both physical and logical. The personnel and physical/worksite security are typically two distinct functions. Giving one office responsibility for both creating policies and procedures for managing physical access ensures that only previously cleared individuals and cleared visitors will gain access to a secure facility or restricted areas.

A state agency will have considerably fewer resources available and physical separation of networks will not be an option. In this instance, the agency must assume that the entire network is certified to contain confidential and proprietary information and build logical controls instead of physical, such as creating secure enclaves. As users of all clearance levels are provided access to the same physical systems, applying the concept of defense in depth becomes critically important to mitigate any gap. Exceptions may be with state military departments (National Guard), law enforcement, and other agencies that exchange classified data with a federal agency. These situations will follow federal standards for information system design.

3.3 Ongoing training

Annual training may be enough for some employees, but is inadequate for those in medium and high-risk positions. This serves several purposes:

- Ensuring that employees are constantly aware of security and privacy issues.
- Reinforcing positional responsibility.
- Promoting professional development and operational readiness.

Strong leadership often includes the intangible qualities of human nature. Should a manager feel reasonably comfortable with an employee who has passed the background check? Yes, but mistakes happen, people change and relying on this alone may not provide adequate assurance. Essentially, the clearance sets the bar high, and employee training and awareness programs keep it there.

If mitigating risk is your goal, and not simply checking the "agency compliant" box, it is much wiser to implement a holistic training program that targets the roles and responsibilities in the organization.

4 Conclusion

Our civil service system, and the whole concept of the American dream for that matter, is based on the idea that we live in a meritocracy. There was a time when nepotism and corruption ran rampant in the federal government. While we will probably never see a federal holiday honoring President Chester A. Arthur, he is responsible for setting the foundation for the public trust concept. In 1883, Arthur signed the Pendleton Civil Service Reform Act, ushering in civil service reform. Prior to this landmark legislation, government jobs were seen as gifts for political supporters. The law ensured that government jobs would be awarded on the basis of merit, thereby ending the spoils system (Karabell, 2004).

How does a reference to an obscure reconstruction-era president fit in to the context of this subject? Over 130 years ago, legislators (from both sides of the political aisle) recognized that patronage in government is a threat to our democratic system. Thus, leaders have a duty to ensure that the most qualified individuals are employed by the government. For a sensitive position, the qualification can include much more than just education and experience. By establishing definitive and reasonable job requirements and ensuring that the risk level of the position is stated in the job description, it ensures that employees and applicants are well aware of what is expected and therefore management can set high standards – a win for both parties.

Information security leaders use a risk management framework to solve problems and make independent and objective decisions. Extending these concepts to personnel security programs makes the decision clear. The personnel security programs employed at the federal level can fulfill the needs of public agencies at virtually all levels. Where state agencies are handling national security information and interacting with federal agencies, a federal clearance will already be required as a contingency of sharing data.

Impinna, joseph.impinna@ftb.ca.gov

6 References

Code of Federal Regulations. (2012, January 1). Designation of public trust positions and investigative requirements. *Section 731.106*. Office of Personnel Management.

Cole, E. (2014). *Insider Threats in Law Enforcement.* Bethesda: SANS Analyst Program.

Dignan, L. (2015, April 2). *Snowden, PRISM fallout will cost U.S. tech vendors $47 billion, less than expected*. Retrieved from ZDNet: http://www.zdnet.com/article/snowden-prism-fallout-will-cost-u-s-tech-vendors-47-billion-less-than-expected/

DNI. (2008, October 8). Intelligence Communicty Policy Guidance. *ICPG 704.2*. Director of National Intelligence.

Earley, P. (1988). *Family of Spies.* New York: Bantam Books.

Exec. Order No. 10450. (1953). *18 FR 2489(1949-1953 Comp), 3 CFR*, 936.

FCRA. (1970). Fair Credit Reporting Act. *PUBLIC LAW 91-508 Title VI*. Retrieved from http://www.gpo.gov/fdsys/pkg/STATUTE-84/pdf/STATUTE-84-Pg1114-2.pdf

GAO. (September 2014). *PERSONNEL SECURITY CLEARANCES: Additional Guidance and Oversight Needed at DHS and DOD to Ensure Consistent Application of Revocation Process*. Washington, D.C.: United States Government Accountability Office.

Gellman, B., & Soltani, A. (2013, October 9). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post*. Washington D.C. Retrieved from http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

Gordon, M. R. (1987, April 16). WEINBERGER SAYS THE WALKERS GAVE SOVIET MUCH KEY DATA. *New York Times*. New York, NY.

Grand, G. (2013, June 22). *Edward Snowden: A Private Contractor Gave Snowden His Security Clearance — and Missed the Red Flags*. Retrieved May 7, 2015, from Mic.com: http://mic.com/articles/50417/edward-snowden-a-private-contractor-gave-snowden-his-security-clearance-and-missed-the-red-flags

Hardy, P. (2006). *Civil Service: Some Pros, Cons and Suggestions for Reform.* Knoxville: Municipal Technical Advisory Service.

Henderson, W. (2007-2011). *FEDERAL SECURITY/SUITABILITY CLEARANCE CHART*. Retrieved May 6, 2015, from Federal Clearance Assistance Service: http://fedcas.com/wp-content/uploads/2012/05/Federal-Suitability-Security-Clearance-Chart.pdf

Henderson, W. (2011, August 7). *How Much Does It Really Cost to Get a Security Clearance?* Retrieved from ClearanceJobs.com: http://news.clearancejobs.com/2011/08/07/how-much-does-it-really-cost-to-get-a-security-clearance/

Hosenball, M. H. (2013, June 20). *U.S. contractor that vetted Snowden is under investigation*. Retrieved from Reuters.com: http://www.reuters.com/article/2013/06/21/us-usa-security-usis-idUSBRE95J13120130621

Hubert, K. (2014). *Evidence Collection From Social Media Sites.* Bethesda: The SANS Institute.

Infosecurity Magazine. (2013, February 21). *A hacker's dream: two-thirds of SharePoint users have no security policy*. Retrieved from infosecurity: http://www.infosecurity-magazine.com/news/a-hackers-dream-two-thirds-of-sharepoint-users/

Joyner, J. (2013, February 21). *Our Stupid Security Clearance System*. Retrieved from Outside the Beltway: http://www.outsidethebeltway.com/our-stupid-security-clearance-system/

Karabell, Z. (2004). *Chester Alan Arthur.* New York City: Times Books.

Kyzer, L. (2014, February 7). *OPM Insources Security Clearance Investigation Reviews*. Retrieved May 7, 2015, from ClearanceJobs.com: http://news.clearancejobs.com/2014/02/07/opm-insources-security-clearance-investigation-reviews/

Ledgett, R. (2013, December 15). NSA speaks out on Snowden, spying. *60 Minutes.* (J. Miller, Interviewer) CBS News. New York. Retrieved from http://www.cbsnews.com/news/nsa-speaks-out-on-snowden-spying/

Mullin, J. (2013, June 12). *NSA leaker Ed Snowden's life on Ars Technica*. (Conde Nast) Retrieved May 18, 2015, from Ars Technica: http://arstechnica.com/tech-policy/2013/06/nsa-leaker-ed-snowdens-life-on-ars-technica/

NCSL. (2015, May 22). *Access to Social Media Usernames and Passwords* . Retrieved June 4, 2015, from National Conference of State Legislatures: http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx

NIST. (2011). NIST Special Publication 800-39. *Managing Information System Risk.*

NIST. (2014). NIST Special Publication 800-53. *Security and Privacy Controls for Federal Information Systems, Revision 4*, control PS-3. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

OPM. (2014, November 4). Implementation of Federal Investigative Standards for Tier 1 and Tier 2 Investigations. *FIN 15-03*. Retrieved from http://www.opm.gov/investigations/background-investigations/federal-investigations-notices/2015/fin-15-03.pdf

Impinna, joseph.impinna@ftb.ca.gov

OPM. (2014, September 29). Investigations Reimbursable Billing Rates Effective October 1, 2014. *FIN 14-07*. Retrieved from http://www.opm.gov/investigations/background-investigations/federal-investigations-notices/2014/fin14-07.pdf

Pike, J. (2000, March 3). *Secret Internet Protocol Router Network (SIPRNET)*. Retrieved from Federation of American Scientists: http://fas.org/irp/program/disseminate/siprnet.htm

Rockwell, M. (2014). Should social media affect your security clearance? *Federal Computer Week, 28*(18), p. 3. Retrieved from http://fcw.com/articles/2014/11/06/odni-social-media-monitoring.aspx

Sontag, S., & Drew, C. (1998). *Blind Man's Bluff.* New York City: Harper Collins.

Suitability and Security Clearance Performance Accountability Council. (February 2014). *Suitability and Security Processes Review.* Washington D.C.: Office of Management and Budget. Retrieved from https://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf

Zetter, K. (2011, December 18). *Forensic Expert: Manning's Computer Has 10k Cables, Downloading Scripts*. Retrieved May 13, 2015, from Wired: http://www.wired.com/2011/12/cables-scripts-manning/

Impinna, joseph.impinna@ftb.ca.gov

7 Appendix A: Recommended state and local agency public trust clearance investigative model

Category	Type of initial investigation	Suitability clearance determination	Reinvestigation
High risk public trust	BI	High risk	Ongoing through continuous monitoring; PRI every five years
Moderate risk public trust	Tier 2	Moderate risk	Ongoing through continuous monitoring; NACLC every five years
Low risk non-sensitive	Tier 1	Low risk	None

Table 2, Recommended state and local agency public trust clearance investigative model

8 Appendix B: Description of investigations

This is a comprehensive list of investigation types used by OPM in conducting background checks, reprinted by permission from Federal Clearance Assistance Service. These services are available to federal customers. State and local customers with a partnership with federal agencies may leverage this system, but entities seeking to establish a public trust clearance outside of the federal system should pattern their own investigation types similar to OPM's structure – with the scope of the investigation being directly tied to the level of clearance requested.

Tier 1 - NAC plus written inquiries to current and past employers, schools, references, and local law enforcement agencies covering the past five years and if applicable, of the appropriate agency for any identified arrests.

Tier 2 - NACLC plus a Personal Subject Interview (PRSI) and written inquires to employers, schools, and references for past five years.

BI (Background Investigation)—NACLC plus a PRSI; interviews at employment, schools, and residences for the past five years; and review of any court actions for past five years.

CREDIT SEARCH - Verification of subject's financial status through a search of all three major credit bureaus covering all locations where the subject has resided, been employed, or attended school for six months or more for the past seven years.

NAC (National Agency Check) - A review of the records of the FBI-HQ (name check), FBI-ID (fingerprint check), SII (OPM's Security and Investigations Index), & DCII (Defense Clearance and Investigative Index), and records of other federal agencies, as appropriate, plus an Interpol records checks on all non-military personnel who resided outside the U.S. for six months or more within the past five to ten years (depending on the type of investigation) or when there is information indicating they may have engaged in criminal activity overseas.

NACLC (National Agency Check with Local Agency Check and Credit) - NAC plus credit search and checks at local law enforcement agencies where the subject has lived, worked, and/or

attended school within the last five years, and if applicable, of the appropriate agency for any identified arrests.

ANACI-P (Access National Agency Check and Inquiries with PRSI) - NACLC plus written inquires to current and past employers, schools, and references covering past five years.

PRSI (Personal Subject Interview) – Interview by an investigator to validate and supplement the data contained in the questionnaire, and clarify or collect additional information relevant to the subject's background, character, reliability, judgment, and trustworthiness. Additional interviews shall be conducted as needed. Sworn statement and other declarations may be taken to assist in resolving issues.

PRI (Periodic Reinvestigation) - NACLC plus PRSI and written inquiries to references.

SSBI (Single Scope Background Investigation) - NAC plus credit search; PRSI; NAC on spouse or cohabitant; interviews at employment for past seven years; interviews at schools and residences covering the past three years; review of any court actions covering the past 10 years; interview of any former spouse divorced within the past 10 years, interview of four social references who collectively cover at least the past seven years; checks at local law enforcement agencies where the subject lived, worked, and/or attended school within the last 10 years, and if applicable, of the appropriate agency for any identified arrests; verification of citizenship or legal status of all foreign-born immediate family members and cohabitant.

Impinna, joseph.impinna@ftb.ca.gov

Last Updated: February 26th, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS London March 2018	London, GB	Mar 05, 2018 - Mar 10, 2018	Live Event
SANS Paris March 2018	Paris, FR	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Secure Osaka 2018	Osaka, JP	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Secure Singapore 2018	Singapore, SG	Mar 12, 2018 - Mar 24, 2018	Live Event
SANS San Francisco Spring 2018	San Francisco, CAUS	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	McLean, VAUS	Mar 17, 2018 - Mar 24, 2018	Live Event
ICS Security Summit & Training 2018	Orlando, FLUS	Mar 18, 2018 - Mar 26, 2018	Live Event
SANS Pen Test Austin 2018	Austin, TXUS	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, AU	Mar 19, 2018 - Mar 24, 2018	Live Event
SEC487: Open-Source Intel Beta One	McLean, VAUS	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Munich March 2018	Munich, DE	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Boston Spring 2018	Boston, MAUS	Mar 25, 2018 - Mar 30, 2018	Live Event
SANS 2018	Orlando, FLUS	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Abu Dhabi 2018	Abu Dhabi, AE	Apr 07, 2018 - Apr 12, 2018	Live Event
Pre-RSA® Conference Training	San Francisco, CAUS	Apr 11, 2018 - Apr 16, 2018	Live Event
SANS London April 2018	London, GB	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Zurich 2018	Zurich, CH	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MDUS	Apr 21, 2018 - Apr 28, 2018	Live Event
Blue Team Summit & Training 2018	Louisville, KYUS	Apr 23, 2018 - Apr 30, 2018	Live Event
SANS Seattle Spring 2018	Seattle, WAUS	Apr 23, 2018 - Apr 28, 2018	Live Event
SANS Riyadh April 2018	Riyadh, SA	Apr 28, 2018 - May 03, 2018	Live Event
SANS Doha 2018	Doha, QA	Apr 28, 2018 - May 03, 2018	Live Event
SANS SEC460: Enterprise Threat Beta Two	Crystal City, VAUS	Apr 30, 2018 - May 05, 2018	Live Event
Automotive Cybersecurity Summit & Training 2018	Chicago, ILUS	May 01, 2018 - May 08, 2018	Live Event
SANS SEC504 in Thai 2018	Bangkok, TH	May 07, 2018 - May 12, 2018	Live Event
SANS Security West 2018	San Diego, CAUS	May 11, 2018 - May 18, 2018	Live Event
SANS Melbourne 2018	Melbourne, AU	May 14, 2018 - May 26, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VAUS	May 20, 2018 - May 25, 2018	Live Event
CyberThreat Summit 2018	OnlineGB	Feb 27, 2018 - Feb 28, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced