THE NATIONAL INFRASTRUCTURE ADVISORY COUNCIL'S FINAL REPORT AND RECOMMENDATIONS ON

THE INSIDER THREAT TO CRITICAL INFRASTRUCTURES

APRIL 8, 2008

THOMAS NOONAN
FORMER GENERAL MANAGER
IBM INTERNET SECURITY SYSTEMS

EDMUND ARCHULETA
PRESIDENT AND CEO
EL PASO WATER UTILITIES

This page intentionally left blank.

Table of Contents

I. ACKNOWLEDGEMENTS

NIAC Working Group Members

Mr. Edmund G. Archuleta (co-chair), President and CEO, El Paso Water Utilities
Mr. Thomas E. Noonan (co-chair), Former General Manager, IBM Internet Security Systems
Dr. Craig Barrett, Chairman of the Board, Intel Corporation
Ms. Margaret E. Grayson, President, Coalescent Technologies, Inc.
Mr. John W. Thompson, Chairman and CEO, Symantec Corporation

Study Group Members

Patricia Alexander, Union Pacific
Peter Allor, IBM and the IT Sector Coordinating Council (SCC)
Larry Brock, DuPont
Robert Clyde, Symantec Corporation
Hal Dalson, CMS Energy and the Dams SCC
Bill Dunne, CME Group
Carla Gore, Dow Chemical and the Chemical SCC
Dan Jenkins, Dominion Resources, and the Oil and Natural Gas (Energy) SCC
Kirsten Koepsel, AIA Aerospace Industries Association and the Defense Industrial Base SCC
Bill Muston, Oncor Electric Delivery
Vijay Nilekani, Nuclear Energy Institute and the Nuclear SCC
John Puckett, DuPont
Bill Ramsey, McCormick & Co., Inc. and the Food and Agriculture SCC
Michael Rossman, McCormick & Co., Inc. and the Food and Agriculture SCC
Vance Taylor, Association of Metropolitan Water Agencies and the Water SCC
Diane Van DeHei, Association of Metropolitan Water Agencies and the Water SCC
Brian Willis, Intel Corporation and the IT SCC
Barbara Wichser, Dominion Resources and the Dominion Resources and the Energy SCC
Stephen Ziehmn, Harris Corporation and the Defense Industrial Base SCC

DHS Support and Resources

Partnership Programs and Information Sharing
Carlos Kizzee
Michael Schooler
Gail Kaufman
Mike Schelble (Contractor, SRA International)

II. EXECUTIVE SUMMARY

The Insider Threat to Critical Infrastructures Study

Charter

Through DHS and the Secretary of the Department of Homeland Security (DHS), the National Infrastructure Advisory Council (NIAC) provides the President with advice on the security of the critical infrastructure sectors and their information systems. These critical infrastructures support vital sectors of the economy, including banking and finance, transportation, water, energy, manufacturing, and emergency services.

Scope

Homeland Security Secretary Michael Chertoff initiated *The Insider Threat to Critical Infrastructures Study* with a letter to the NIAC at the Council's January 16, 2007 meeting. The Secretary's letter outlined a series of tasks, which helped frame the Study. The tasks included defining the insider threat for both physical and cyber; analyzing its scope, dynamics, and the effects of globalization; outlining obstacles to addressing this potential threat; and analyzing the challenges that Critical Infrastructure and Key Resource (CIKR) owners and operators face when they screen their employees for insider threat risk. The NIAC Working Group divided the assigned tasks and the work of the Study Group into two phases. The first phase focused on defining the threat, dynamics, scope, globalization, and obstacles, while the second phase highlighted issues and challenges related to employee screening.

Goals

The NIAC's primary goal was to address the assigned tasks and develop policy recommendations for the President and DHS in an effort to improve the security posture of our Nation's critical infrastructures. The NIAC also sought to leverage its findings to increase understanding of the insider threat and help CIKR operators mitigate insider threats.

Background

Insider threats exist for all organizations. Essentially, this threat lies in the potential that a trusted employee may betray their obligations and allegiances to their employer and conduct sabotage or espionage against them. Insider betrayals include a broad range of actions, from secretive acts of theft or subtle forms of sabotage to more aggressive and overt forms of vengeance, sabotage, and even workplace violence. The threat posed by insiders is one most owner-operators neither understand nor appreciate, and it is a term that is commonly used to refer to IT network use violations. This often leads to further confusion about the nature and seriousness of the threat.

This misunderstanding or underestimation relates, in part, to the stigma that an act of insider betrayal carries with it – a stigma that can cause customers, partners, and shareholders to lose trust in an organization. This loss of trust can translate into lost business, revenue, and value. As a result, CIKR owner and operators often handle these types of events discretely and away from public view. This common practice has impeded the understanding of the threat and the efforts to address it, exacerbating the existing risk.

In its investigation, the NIAC uncovered a significant, and growing, body of knowledge about the causes and implications of the insider threat. The NIAC has compiled a high-level view of these findings in its effort to lift the veil of misunderstanding and, in turn, provide a path forward to mitigate insider threat risks to critical infrastructure.

Findings

The NIAC developed detailed findings, which are included in the report to address the tasks assigned to the Study. These findings also represent a part of the process used to identify gaps for policy solutions. A brief overview of the NIAC's findings follows.

To begin, the NIAC defined the insider threat to critical infrastructure as *one or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm.* The NIAC tested this definition over the course of its investigation and used it to set parameters for explorations and following findings.

The discussion on *Scope* explores the nature and psychology of insider threat perpetrators to provide understanding of the threat's origins, and demystify the process for developing individualized CIKR operator solutions. The NIAC determined insider threats to be significant given their potential to cause serious consequences that cascade beyond the attacked infrastructure. The NIAC also found economic espionage poses a significant threat to the competitive viability of many critical infrastructures in the United States. Additionally, the NIAC found that awareness and mitigation of the threat varies greatly among the critical infrastructure sectors.

The dynamics discussion identifies that rapidly escalating technology and network risks are combining with growing globalization of workforces, supply chains, and service providers to produce new threats and risks. The rapid change and complexity of these two issues limits the specificity that the Study can provide in terms of solutions, but the NIAC's exploration has highlighted gaps and areas of focus future work and research.

The obstacles discussion outlines gaps addressed by the recommendations, including: information sharing, follow-on research, education and awareness, identity management, CIKR employee screening practices, technology challenges, and cultural and organizational challenges.

On the issue of employee screening, the NIAC found current law enables some sectors to screen their employees while leaving others vulnerable. The NIAC found CIKR sectors vary so widely that a cross-sector, homogenized and government-applied screening process would not adequately address the problem. The NIAC found CIKR operators need to assess criminal history records to make their own risk determinations and adjudications.

Recommendations

In the recommendations, the NIAC has outlined significant steps for the President, Congress, Federal agencies and critical infrastructure sector organizations that will improve security against insider threats. These recommendations and suggested approaches intend to focus and optimize CIKR operator resource allocations to achieve elevated insider threat protection. The NIAC found no cases where increased regulation would better achieve this goal. <u>To be clear, none of the NIAC's recommendations should be interpreted as a call for regulation.</u>

The recommendations include low-cost, easily implemented policy solutions for near term effect, and also a path forward to address the poorly understood, complex, and rapidly evolving challenges the NIAC uncovered. The NIAC recommends that policy makers should move swiftly to implement the near term improvements and increase the security of our critical infrastructures. A summary of the NIAC's recommendations follows.

Near-Term Insider Threat Policy Recommendations

Education and Awareness

Finding: the NIAC identified that many CIKR operators lack an appropriate awareness of the threat insiders pose to their operations. Education and awareness presents the biggest potential return for policy by motivating CIKR operators and focusing their efforts to address the insider threat. Appropriate awareness will help to shape the insider threat policies and programs needed to address the unique insider risk profile of each CIKR operator.

The NIAC's recommendations to improve education and awareness include:

1. Establish leadership for national insider threat programs within the Executive Office of the President to coordinate government support for CIKR operator education and awareness of insider threats.
2. This DHS-based program should have the goal of establishing a common baseline understanding of the emerging and dynamic insider threat to critical infrastructures. It should help promote the broad corporate cultural changes needed to elevate internal security and protect against the insider threat. Key elements of this program should include:
    a. leveraging the Executive Office of the President to communicate the issue with executives and partner with companies in each sector to develop pilot programs;
    b. educating executives on key aspects of the insider threat to help in identifying enterprise-level insider threat risks;
    c. assisting CIKR operators in developing insider threat education and mitigation programs; and
    d. identifying and supporting areas for future insider threat research.

The NIAC developed a framework for outreach and awareness and another for best practices and policies. Both frameworks can help develop and implement programs necessary to increase education and awareness of insider threats and solutions for corporate leadership across sectors.

Employee Screening

The second critical area with potential for near-term improvement in insider threat mitigation programs is improved employee screening. Given the increased potential for catastrophic consequences to critical infrastructure from an insider attack, the NIAC found CIKR operators need access to the best available criminal history records for critical employee risk assessments. Many CIKR operators lack access to the fingerprint-based FBI criminal history records required to conduct an accurate threat risk assessments for their employees.

To address this, the NIAC recommends Congress provide CIKR operators with statutory access to FBI criminal history records as a part of a comprehensive program that also includes measures to ensure appropriate privacy protection and appropriate use of these records. The NIAC has outlined the key issues necessary to address this recommendation below.

1. Government should provide uniform statutory access for CIKR operators to Federal fingerprint criminal history records to improve accuracy of employee risk assessments.
2. To accommodate the diversity of CIKR operators, implementation should avoid a one-size-fits-all approach. This program should provide CIKR operators discretion to: choose when to participate and screen employees; review and assess employment candidate criminal history records directly (subject to Federal and State legal restrictions); establish their own adjudication criteria to meet differing levels and types of risk; and use the program to screen current and prospective employees on an as-needed basis. The measure

should also provide access for the regulated third-party background screening companies that some CIKR operators use in their screening processes.

3. To protect individual privacy rights, this program should adhere to existing FCRA privacy standards for criminal history checks in the private sector. Most importantly, these protections should include the rights of an individual to do the following:
    a. authorize any check of their records; review, challenge, and correct inaccurate information on their record; and appeal a decision based upon inaccurate information.

    Privacy protection requirements for information users should include:
    a. standards for handling and protecting privacy information; clear limitations on use and dissemination of privacy information; criminal penalties for negligent use or misuse of information; user enrollment agreements, similar to those used with law enforcement organization access; and user program compliance audits.
4. To maximize the accuracy of the information used for employment screening, programs implemented to screen CIKR employees should:
    a. fund measures to improve the accuracy of records;
    b. standardize the presentation of records;
    c. include programs to educate users on how to read RAP sheet records; and,
    d. when possible, be conducted by an agency in the State of employment and, when not possible, by a Federal agency.
5. Legislation should provide long-term funding through use of fees and include appropriation for a near-term solution, balancing the needs of all involved Federal and State entities.
6. As incentive for CIKR operators to support ex-offender reintegration policy, the program should include measures for liability protection when employers hire a candidate on terms that meet a national set of fair use guidelines.
7. To improve the value of information provided to CIKR operators through this program and to help develop guidelines to protect individuals from undue employment discrimination, government should conduct research on the nexus between criminal history and insider risk, as outlined in the research recommendations. This research should refine the national fair use guidelines described in the recommendation above.

Technology Policy

The complexity of technology challenges requires further research and work in many areas, but the NIAC identified several near-term policy solutions as well. The following recommendations will help mitigate risks to technology infrastructure from an inside attack:

1. CIKR operators should establish a priority to maintain current network/IT security best practices.
2. To improve CIKR worker ethics, accountability, and understanding of appropriate IT network conduct, the NIAC recommends the following:
    a. secondary education training on ethics and awareness of the real consequences of cyber actions for future workers;
    b. improved accountability for virtual crimes through prosecution and equitable punishment for the tangible consequences of cyber crimes;
    c. Greater CIKR operator established and enforced network accountability with stronger identity management tools, and worker education programs.

Information Sharing

NIAC recommendations also addressed gaps in information collection, sharing and analysis on insider threats. Policy implementation should emphasize recommendations with the potential for a near-term effect.

The NIAC found the perceived gap in insider threat awareness and security focus among CIKR operators has emerged, in part, from a lack of usable information on insider threats. CIKR operators need improved information sharing to help inform their insider threat security investment decisions. The NIAC's recommendations to improve information sharing on insider threat, risk, and mitigation include the following:

1. Government should create a clearinghouse resource for owner-operators to assist in the assessment and mitigation of their insider threat risks, leveraging the structures in the Education and Awareness recommendation as well as the accompanying Report Appendices.
2. Government should establish a mechanism to communicate intelligence agency understanding on insider threats, making use of cleared personnel in each sector and provide periodic, useful briefings on developments about insider threats.
3. Government should develop a mechanism and validated process to share information on national security investigations in order to address a specific information-sharing obstacle identified by the NIAC between government and critical infrastructure owner-operators.
4. Each sector should establish a trusted process and mechanism to share incident information on insider threats in a protected manner. Protected information can be aggregated anonymously to inform CIKR risk assessments in all sectors.

A Path Forward: Follow-on Insider Threat Study and Research

Time, resources, and current understanding of the insider threat limited some of the NIAC's recommendations. For these areas, recommendations focused on outlining a path forward with areas for future research by properly resourced groups and organizations.

The primary issue requiring future study relates to risks from globalization. The NIAC found that much of the current research on the insider threat lacks validity in international environments, which makes the risk involved there less quantifiable. To date, studies have focused on developing findings for domestic U.S. employers and the U.S. government. To ensure the security of U.S. critical infrastructures, global CIKR operators need further research on multinational operating environments to be able to assess these risks accurately.

In addition to the need for research into risk, global companies require guidance if they are to develop strong multinational mitigation programs. For global CIKR operators, variation among international legal environments presents another challenge, employee screening being the most obvious. Employers often have few means of verifying identity and assessing risks for overseas employees. The Study's investigations explored this problem, but the NIAC was unable to identify a policy solution that could be implemented readily. Future work is required to address this issue.

Research

Research is required to develop proper mitigations, policy, and goals in the areas of global workforces, criminal history risk assessment, and technology challenges. Specifically, the NIAC identified the following critically needed areas of study:

1. Research insider threats in the context of globalization and the effects of outsourcing, global operations, and diversifying work forces.
2. Research the intersection between a history of criminal convictions and employee behavior, including insider threats to help to improve risk assessments for CIKR

operators and shape policy that will protect against unreasonable employment discrimination.

3. Government should leverage the findings of the recent Defense Science Board Report to address hardware and software assurance issues, which are of critical importance to CIKR operators and carry potential for massive insider threat consequences.
4. Government should convene a steering group of IT technology experts to explore technological solutions to the insider threat in the following areas:
    a. Improved identity management technologies and tools to create a strong, persistent, portable, and platform independent secure network and physical access identity for CIKR workers.
    b. Improved information protection technology applications to assist in the protection of CIKR operator sensitive data through development of stronger, persistent, and more useful data protection tools or *mandatory access control* tools.
    c. Improved cross-platform insider threat data correlation tools, to assist CIKR operators in identifying anomalies and insider threat-related behavior patterns across heterogeneous IT systems and physical access systems.
    d. Continued development of network/IT psychometric tools to improve threat identification and understanding.
    e. A systematic risk management IT insider threat mitigation approach to assist developers and CIKR operators in their processes.
    f. Examine emerging trends and develop guidelines for technologies to mitigate insider sabotage through IT systems management, which because of its level of access, carries potential for widespread and disastrous consequences.

Further Guidance, Findings, Samples, and Tools

The NIAC also developed appendices with suggested guidance on approaches for CIKR operators and policy makers. Appendix B outlines the NIAC's findings that are usable as guidance for increasing awareness among CIKR executives. Appendix C, the Insider Threat Best Practices framework, provides an overview of the techniques and methods uncovered by the NIAC, presented in a risk controls framework approach. CIKR operators can use this approach as a framework for developing their own tailored insider threat program.

Conclusion

The Insider Threat Study, like other NIAC studies before it, found that partnership and information sharing are key components to the success of critical infrastructure protection. Success in information sharing is dependent upon building an ever-stronger public-private partnership and establishing trusted relationships among the key players in each sector and with the government. The partnership to protect critical infrastructure must be grown and strengthened if these efforts are to succeed.

III. BACKGROUND ON THE NIAC

Through the Secretary of the Department of Homeland Security (DHS), the NIAC provides the President with advice on the security of the 18 Critical Infrastructure and Key Resource (CIKR) sectors and their information systems. These CIKR sectors span the U.S. economy and include the Banking and Finance, Transportation, Water, Energy, and Emergency Services Sectors. The NIAC also advises the lead Federal agencies that have critical infrastructure responsibilities and industry sector coordinating mechanisms. Specifically, the council has been charged with:

- enhancing cooperation between the public and private sectors in protecting information systems supporting critical infrastructures in key economic sectors and providing reports on the issue to the President, as appropriate;
- enhancing cooperation between the public and private sectors in protecting critical infrastructure assets in other key economic sectors and providing reports on these issues to the President, as appropriate; and
- proposing and developing ways to encourage private industry to perform periodic risk assessments of critical information and telecommunications systems.

IV. BACKGROUND ON THE INSIDER THREAT STUDY

Homeland Security Secretary Michael Chertoff initiated the NIAC's *Insider Threat to Critical Infrastructures Study* with a letter to the Council on January 16, 2007. In his letter, Secretary Chertoff asked the NIAC to study the Insider Threat in the context of critical infrastructure protection. The Secretary also provided guidance on the issues the Department needed addressed. This guidance, which is outlined below, served as a framework for the seven tasks that make up this Study.

1. Define the "insider threat" both physical, cyber, and examine the potential economic consequences.
2. Analyze the dynamics and scope of the insider threat, and critical infrastructure vulnerabilities.
3. Define the obstacles to addressing the insider threat.
4. Analyze the potential impact of globalization on the critical infrastructure marketplace.
5. Identify issues, potential problems, and consequences associated with screening employees.
6. Identify legal, policy, and procedural aspects of the issue, as well as any potential obstacles, from the perspective of the owners and operators.
7. Develop policy recommendations on potential remedies, up to, and including, possible legislation.

V. APPROACH

The NIAC began by consulting the White House for guidance on the best approach to identify the CIKR sectors most vulnerable to an insider breach. After careful consideration, the NIAC elected to study the following sectors: Banking and Finance, Chemical, Commercial Facilities,

Dams, Electricity, Defense Industrial Base, Food and Agriculture, Information Technology (IT), Nuclear, Oil and Natural Gas, Transportation, and Water. In turn, the Working Group, through the assistance of PCIS, engaged the Sector Coordinating Council (SCCs) from the aforementioned sectors and the respondents formed the Study Group. Each relevant SCC chair nominated security experts from their respective sectors to assist in the Study.

The Working Group split the Study into two phases. The initial phase focused on defining the insider threat. Members then turned their attention toward a thorough examination of the scope, dynamics involved, obstacles to mitigation, as well as the effects of globalization. The Study's second phase focused on legal, procedural, and policy barriers for private sector infrastructure operator employee screening efforts. The Study Group conducted work on the tasks by holding weekly conference calls and quarterly face-to-face workshop meetings to explore the issues. The Working Group completed Phase I research in October 2007, before beginning work on Phase II, which focused on screening, legal obstacles, and potential recommendations. The Working Group delivered its final report to the full NIAC for deliberation and approval in April 2008.

The NIAC drew upon subject matter experts, previous NIAC recommendations, related research, and existing programs to set the scope of the inquiry and develop recommendations for cyber and physical insider threats to critical infrastructures. Initially, the group focused on developing a common cross sector definition for the insider threat to frame the follow-on exploration of *scope, dynamics, globalization and obstacles.* The NIAC developed policy recommendations on mitigating the insider threat and its impact on all critical infrastructures. The NIAC also sought to address regulatory and legal issues to provide a clear legal environment for CIKR owner-operators in their ongoing efforts to protect our Nation's infrastructures.

VI. PHASE I – FINDINGS

A. Defining the Insider Threat

In his letter to the council, Secretary Chertoff asked the NIAC to define the "insider threat" for physical and cyber. In addition, the Secretary asked the council to include an analysis of the potential economic consequences associated with the insider threat.

To address the Secretary's request, the NIAC developed a working definition for the insider threat to critical infrastructures. The NIAC applied and tested this definition throughout the Study, and the definition helped shape policy recommendations for addressing the insider threat. The following is the outcome of the Study's development and testing process for a definition of insider threat to critical infrastructures:

> *The insider threat to critical infrastructure is one or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm.*

In its deliberations on the definition of the insider threat, the NIAC carefully considered the importance of *access* – access to the systems, facilities, or information where an infrastructure's vulnerabilities lie. Inclusion of all people with access expands the group of potential insiders

beyond company employees, to include unescorted vendors, consultants, and contractors with access to an infrastructure's facility or IT system.

Largely, employers grant access to individuals based on trust. For critical infrastructure (CI) owner-operators, the level of established trust and the safeguards for its verification must be scaled to an employee's knowledge of, and access to, the infrastructure's vulnerabilities and critical assets.
Therefore, an employer must base an effective trust relationship with an employee on the following criteria:

1) Establish an appropriate level of trust at employment;
2) Create effective compliance monitoring to ensure established trust is valid over time; and
3) Revoke access, in a timely and effective manner, when the employee has violated that trust.

In the definition above, *inside knowledge* encompasses those former employees who might lack current access but might have retained knowledge of potential security measures or vulnerabilities. In addition, it includes non-employee individuals with access. *Inside Knowledge* also draws emphasis to those mission-critical positions within a company where an employee's access, combined with knowledge of systems and vulnerabilities, creates the greatest potential for harm from an insider attack.

The NIAC also considered the potential for combined physical-cyber attacks. Although physical and cyber threats from insiders manifest differently, the concepts are quickly converging as many potential attacks bear characteristics of physical and IT sabotage, fraud, or theft. Given the intertwined nature of these threats, adequate protection against insider threats requires converged physical and IT security systems and policies. Further, a coordinated attack that combined and leveraged an insider attack with an external attack would carry the potential for multiplier effects and far greater consequences than a simple one-dimensional attack.

To varying degrees, critical infrastructures depend upon each other to deliver services. In developing their recommendations, NIAC members sought to acknowledge and account for these critical interdependencies. Mitigation efforts need to account for worst-case scenarios because attackers can time or leverage their assaults with outside attacks in order to create the most devastating effects. Currently, policy makers lack an effective model to estimate the economic effects of critical infrastructure service interruptions, including those generated by insider attacks.

B. Scope and Dynamics

In his January 16 letter, Secretary Chertoff asked the NIAC to analyze the dynamics and scope of the insider threat and assess critical infrastructure vulnerabilities to the insider threat.

Scope

The NIAC considered a broad set of factors before determining the scope of the insider threat to critical infrastructures. To determine its findings, which are outlined below, the NIAC examined the following four questions in detail:

- What level of consequence constitutes an infrastructure-level threat?
- What is the range of potential insider actions that could harm critical infrastructures?

- Who are the potential actors in this type of threat, and what are their motivations?
- How do these factors contribute to improving risk mitigation for insider threats?

After considering the broad spectrum of insider threats faced by critical infrastructure owner-operators, the NIAC focused squarely on those threats with the potential to interrupt delivery of CIKR services. Lesser threats to CIKR operators, while troublesome, do not fit within the context of the risk management approach used by CIKR operators to set policy and make security investment decisions. From a public-policy standpoint, these critical infrastructure-level threats carry potential for psychological effects, including a loss of public confidence in government, institutions, and/or services. Moreover, these threats have the potential to cascade from their point of origin to affect broader regions and other critical infrastructure sectors.

The NIAC found critical infrastructure-level threats include the following consequence scenarios:

- interruption of critical infrastructure services to a geographic area or sector;
- large scale economic loss caused by: physical damage and financial loss; financial failure of a CIKR service provider; loss of critical intellectual property or technology, causing loss of economic competitiveness and as a result, ability to maintain delivery of critical infrastructure services;
- psychological effects including loss of public confidence in services, institutions, or government, which could lead to large scale economic loss; and
- loss of life or compromise to public health.

The study also found instances where the effects of critical infrastructure-level events cascaded to larger geographic areas and other infrastructures, often times resulting in serious adverse economic effects.

Preventing all insider threats is neither possible nor economically feasible. Effective and practical programs designed to address insider threats will use good risk management strategies. Such strategies will begin by identifying a company's physical and intangible critical assets. From a public policy perspective, the greatest threats would affect public health, public psychology, and economic activity. In many cases, interruption of critical infrastructure services would cause all of these. However, from the perspective of critical infrastructure owners and operators, the greatest risks are those threats that would negatively affect their critical assets, such as systems vital to operations, systems that deliver services, or the facilities where those systems are located. Critical assets can also be intangible; examples include brand-image, public confidence in product or services, or anything that affects market share and shareholder value. There is a clear overlap between owner-operator and public policy concerns, as it is clear that both place the highest value on delivery of Critical Infrastructure (CI) services. Effective corporate risk management of critical infrastructure owner-operator risks will address greater public policy concerns, protecting public health, public psychology, and stable economic activity.

Companies affected by insider betrayals suffer losses due to IT or physical sabotage, theft or fraud, or, increasingly, intellectual property (IP) theft, otherwise known as economic espionage.[1]

[1] The Economic Espionage Act (18USC Section 1831-1839) applies solely to the theft of commercial trade secrets, but the study found that all CIKR companies have critically valuable information that, if stolen could threaten their

Each of these attacks has the potential to interrupt a critical infrastructure operator's ability to deliver services. Physical and IT sabotage have an obvious and direct connection to worker and public safety, public health, and the potential to interrupt delivery of critical infrastructure services to the public. Sabotage to operations, safety systems, or the computer systems that control operation of CI services distribution clearly can cause harm or bring CI service delivery to a halt. Theft, fraud, and economic espionage also carry the potential to interrupt delivery of CI services, albeit in a less direct manner. These acts can weaken or destroy public trust, share value, and financial solvency, all of which are necessary for a company to operate. These types of insider betrayals can slowly erode or precipitously destroy the financial foundations of a company and disrupt its ability to deliver CI services.

Potential Actors and Motivations

Insider risk mitigation begins with a complete understanding of potential insider threats. This understanding must include a thorough assessment of potential malicious actions, the types of potential actors, including their capabilities to cause harm and interrupt CI services, and the possible motivations of these individuals.

Individuals responsible for insider betrayals can be labeled as one or more of three different types of actors: 1) psychologically-impaired disgruntled or alienated employees;[2] 2) ideological or religious radicals; and 3) criminals. Moreover, insiders are very often identifiable by more than one of these categories. Identifying these different types of actors is important in understanding insider actions and developing effective programs to mitigate insider risks.

Given the types of potential actors, there are corresponding motivations, which do not necessarily correlate to the characterization of the actor. Motivations for insiders can be summarized as some combination of: revenge for a perceived wrong; radicalization for advancement of religious or ideological objectives; or simple illicit financial gain.

It is important to note that many employees with motivation and malicious intent never commit acts of betrayal. The inhibitions to betrayal can range from simple and readily identifiable, such as avoidance of adverse consequence, to more complex and less obvious motivations, which could include motivations such as attachment or devotion to a specific individual. Alternatively, those who do commit malicious insider actions most commonly have a causal experience or mechanism to betrayal. These mechanisms or causations to malicious action can be categorized as coming from three different sources: 1) growing, exacerbated or unaddressed discontent with their place or value in the organization; 2) recruitment by hostile outside entities or groups; or 3) infiltration of a malicious actor to a trusted position on an infrastructure operator's staff.

An important concept to note with these descriptors is the subset of the passive or *unwitting* insider. Unwitting insiders are easily manipulated employees, who, for similar reasons and motivations to active insiders, are recruited to divulge secrets or critical information about a company by a malicious third party. Passive and unwitting insiders range from individuals who

---

ability to operate. As a result, the study uses the term to refer to the broader application of this critical information that is being stolen from these companies.

[2] This category of insider proved a difficult point to communicate and was originally termed as simply *disgruntled*, which proved to be inaccurate as a label. The terms used here are intended to be descriptive – insiders fit the description, but not all fitting the description have the potential to be insider threats.

share information, blissfully unaware of their exploitation, to those who are manipulated into compromising positions and coerced into varying degrees of more active betrayal.

Anonymity and accountability also play a significant role in many malicious insider actions. Insider studies have shown that violators are averse to being caught and are more likely to act when they believe they will not be discovered. Successful insider threat programs have shown that establishing clear accountability for actions and setting expectations and boundaries for employee conduct have significant potential for mitigating effect, even when employers believe an individual is near to taking malicious action.[3]

Each of the points raised here – actor-types, motivations, mechanisms, accountability – represent opportunities to mitigate potential insider threats. Understanding the interplay of these factors in insider risk is important to developing cost effective, organization- and sector-specific, targeted risk mitigation programs that will effectively protect the financial stability of CIKR operators and delivery of their critical infrastructure services.

The insider threat actor types are intended as descriptions and individuals can be seen as belonging to more than one of these groups. Criminal actors are individuals who often possess criminal records or associate with criminal organizations. These actors exploit their employment position for illicit financial gain through theft, fraud, or more complicated financial schemes. Religious and ideological radicals are individuals consumed with advancing the goals of their ideology or religion and violate the trust of their employer for that purpose. The process of radicalization is often dynamic and it can occur after the employee has gained the trust of his employer. A variation on the criminal type, economic spies use their position and knowledge to sell or give valuable intellectual property to interested, competing countries, or companies.

In cases where an organization has been targeted for infiltration, the NIAC discovered that a process of rigorous background investigations could significantly mitigate the risk of nefarious outside infiltration. However, success in this approach is likely to shift the focus to attacks based on recruitment, radicalization, or compromise of trusted employees. Further, recruited insider involvement can span a range of motivation and involvement from active betrayal to less obvious forms that include passive, unwitting, or unwilling involvement. Effective mitigation strategies must address these different types of risk and attack profile, because each includes potential serious consequences for an infrastructure owner-operator.

Psychology of the Insider

Understanding the psychological factors that shape insider behavior is critically important to understanding the threat. Current research indicates this psychological model might play a role in virtually all insider threat cases, even those where ideology, religion, radicalization, and crime play a central role.[4] Because the psychological model for describing insider behavior can potentially be applied to all insider threat cases, an opportunity exists to use these common indicators to cover a broad array of threats in risk mitigation strategies and prevent insider incidents before they happen.

---

[3] Concept discussed with Dr. Eric Shaw, on July 8, 2007 and September 10, 2007 and Dawn Cappelli of CERT on July 30, 2007.

[4] As noted in the following paragraph, CERT's 2006 report, titled *Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis* showed psychological commonalities between IT Sabotage and Government Espionage cases.

Carnegie Mellon's Computer Emergency Response Team (CERT) organization, in coordination with the U.S. Secret Service National Threat Assessment Center (NTAC), has conducted several extensive research projects on insider threats. A December 2006 report, *Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis,* compared data gathered on IT sabotage insider cases with a model developed from analysis of recently compiled U.S. espionage cases. While the data set available for this work was not large enough to constitute a truly scientific study, this, along with CERT's other recent work, is the most instructive research and detailed data set available to date. Models in this study showed there were significant commonalities between spies and IT sabotage cases. The CERT study also revealed a common set of personality traits or pre-dispositions for insider betrayals and a model for their behavior that shows how their behavior deviates from what management would expect from a typical employee in a similar situation. In addition to discussing the findings of the CERT Study with researcher and author Dawn Cappelli, the NIAC also met with clinical psychologists, Dr. Eric Shaw and Dr. Michael Gelles. Discussions revealed that although there are minor differences of perspective on specific points around the common psychology of the insider threat, each of these experts agreed that insiders share common personality characteristics and a similar path to betrayal of trust.[5]

Leading researchers in the field describe potential insiders as being a difficult or high maintenance employee with several characteristics that indicate a predisposition for insider betrayal. These characteristics include personality issues that affect social skills and decision-making with a history of rule violations, and can include social network risks and medical/psychiatric issues, including substance abuse.[6] Rather than being a profile for insiders, this is the first set of indicators in what is termed a "critical pathway." These factors interfere with an individual's ability to adapt to or handle stress in a normal manner, and in conjunction with a series of steps and events, can sometimes lead to malicious insider action. The other common finding from the existing research was the precipitating role of stressful events or "stressors." These stressors, whether from work, home, or life in general, precipitated malicious acts of betrayal in most of the studied insider threat cases. In many cyber sabotage cases, misguided interaction between management and the individual was the specific cause that led to the act of betrayal.[7]

Discussions on insider threat betrayals often describe insiders as disgruntled, and while this is a convenient and somewhat accurate stereotype, it is limiting in the sense that the insider psychology is more complex. This oversimplification could mislead insider threat programs to focus on disgruntled employees. Despite the appearance of contrary evidence, there is no direct correlation between disgruntled workers and insider threats. The majority of disgruntled employees, even those with insider predispositions, never come close to betraying their employer.

---

[5] Carnegie Mellon's Software Engineering Institute CERT program has developed an extensive set of resources on insider threats, which are available at: http://www.cert.org/insider_threat/.

[6] Ideas presented in a brief to the Study Group titled: *Support to the NIAC on The Insider Threat: Findings, Implications, Innovations,* by Dr. Eric Shaw on July 12, 2007, slide 13.

[7] *Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis,* 2006, pages 19-20.

However, in cases where betrayals occur, management and/or human resources were well aware of the employees and their issues in advance of the incident.[8] Each of the factors in the insider psychology model represents an opportunity for intervention and mitigation before a situation reaches a calamitous violation of trust.

While there is a lot of encouraging research on insider behavior and how these threats can be addressed, the area still needs more research. The NIAC found the psychological model for insider behavior needs further development – especially concerning cases involving ethnic nationalism and economic espionage.[9]

Economic Espionage

The most significant, and perhaps least anticipated, finding of the Study is the large and growing threat of Nation-State economic espionage targeting critical technologies in U.S. critical infrastructure companies. While this threat does not carry an immediate and direct threat to the ability of infrastructure owner-operators to deliver CI services, the potential for financial losses is enormous. Unchecked, this threat would undermine the competitiveness of these companies and could potentially drive them out of business. In sectors where operators own high-value intellectual property, efforts to address the insider threat must include measures mitigating intellectual property theft and protecting these vital assets.

Of the economic espionage threats, the threat posed by Nation-State actors seeking critical U.S. technologies is the most serious. Many countries have vast technical resources, highly sophisticated tools, deniability, and a significantly lower level of accountability than individuals or competing corporations. State-sponsored espionage often ties in with corporate espionage, feeding stolen technologies to domestic companies in direct competition with the espionage target. Infrastructure operators will need coordination, threat information, and governmental assistance to protect against this threat properly.

Economic espionage is not always State-sponsored. Dynamics in workforce markets are raising the rates of employee turnover, which in turn, increases the exposure of companies to IP loss and the likelihood that their high-value institutional knowledge could be transferred to a competitor or nefarious outside interest. Today, the loss of intellectual property through employee turnover is common and represents a significant risk factor for CIKR companies. Recent technological developments, such as miniaturization of data storage, have the potential to magnify this risk. To be effective, insider risk mitigation programs must include measures to protect high-value intellectual property. Effective policy and technology-driven IP protection programs will also address the risk represented by employee turnover to some degree.

Variation among the Sectors on Maturity and Awareness

Awareness of the insider threat varies greatly among the critical infrastructure sectors. Strong examples include the Banking and Finance as well as Nuclear sectors, which have an excellent awareness of the threat as well as robust risk mitigation approaches to insider sabotage and

[8] Dr. Eric Shaw, in his presentation to the Study Group noted that research has discovered no "big bangs" - cases where an employee violated trust without prior indicators or warning.

[9] Clinical Psychologist, Dr. Michael Gelles attributed many of the economic espionage cases to a psychological factor he called "dual identity," a pattern where an individual and their allegiances were divided between two groups or communities, making them prone to betray their employer for the other.

insider fraud. Other sectors have varying levels of awareness and risk mitigation programs. There is even significant variation within some of these sectors. While the NIAC found some, mostly larger, operators in the IT and Chemical sectors who have developed strong, focused insider threat programs, it is clear many others have not. Some factors that appear to be stalling action include greater competition and less cooperation among owner-operators in a sector and less-coordinated and less-cooperative relationships with labor workforces. These companies often have externally-focused security policies with more tangible, identifiable objectives.

Among those companies that are not managing insider risks, owner-operator understanding of the threat is the primary problem. Misperception of the risk can result in complacency and denial about the insider threat. Surveys have shown corporate leadership understands that insider incidents occur, but it appears corporate leadership neither completely appreciates the risk nor realizes the potential consequences.[10] As a result, most companies do not actively manage their insider risks.

Infrastructure owner-operators are willing to address these risks when the threat is understood clearly and mitigation goals are achievable and cost effective. CIKR operators lack and critically need a comprehensive, systematic means to identifying the full spectrum of insider threats. A comprehensive understanding of the threat through improved information sharing, research, and effective communication of threat information to decision makers will go a long way toward addressing this gap in the less-regulated infrastructure sectors. Further, owner-operators need communication of effective approaches to insider threat risk mitigation with scaleable, adaptable solutions for operators of different sizes.

Currently, companies that have experienced insider incidents are reluctant to share this information because of the costs involved – insider incidents can cause lost credibility with shareholders, employees and customers, and negatively effect to shareholder values. Without mature, comprehensive business intelligence-level information, leadership will be unlikely to see the insider threat as the enterprise-level risk that it is and invest to manage it proactively.

Dynamics

The NIAC found that rapidly escalating technology and network risks combined with the dynamic of globally distributed workforces, supply chains, and service providers has produced serious, emerging, and evolving insider threats.

To begin, industry at large is immature at detecting malicious insiders. Currently, most insiders are discovered after they have already committed a costly malicious act. While there are efforts ongoing, few sectors or companies have strong, research-based programs designed to detect malicious behavior before it happens. Until recently, there has been little focus on the insider threat and useful research has only emerged in the last three years. The need for effective insider threat programs is escalating due to the emerging globalization and technology/network threats.

Technology Dynamics and the Insider Threat

Transformations in workforce dynamics driven by the rapid pace of technology advancements will continue to have profound effects on the threat posed by insiders and need to be considered

[10] Based on Study Group assessment of survey data, such as the 2007 Computer Crime and Security Survey from the Computer Security Institute.

in planning risk mitigation programs and policies. Technology risks for companies are escalating rapidly.

Proliferation of small, mobile computing devices and the ubiquitous nature of Internet access have eroded traditional workplace boundaries. Increasingly, virtual work environments are replacing static workplace boundaries, a reality that is, in turn, pushing toward decentralization and expanding a company's attack surface. In addition, increasingly miniaturized storage and computing devices increase the capability of an insider to steal data or introduce malicious software into a company's network environment.[11]

Advances in system management and automation tools have increased the breadth and reach of an insider attack. New business models and software tools now allow a single individual to manage many platforms that can be located around the globe. Not only does this magnify the potential impact of a malicious insider, it also expands a company's threat exposure as these privileged system and network administrators can be positioned outside the United States.

The role of globalization adds another layer of complexity to the issue of trust and collaboration. Technology and business process collaboration are making the world increasingly inter-connected. Often design, engineering, and manufacturing are collaborative efforts involving a robust interchange of people, process and systems. As one's 'web of trust'[12] expands to include these collaborative partners, a company's attack surface and threat space (system vulnerabilities, types of attacks and potential attackers) increases exponentially.[13]

Technology is also driving generational cultural issues as well. The pervasiveness of technology is changing the next generation workers and potential insider threats. New employees entering the workforce are more comfortable with technology and have expectations for persistent connectivity to friends, family, and fellow workers. CIKR operators seeking to implement improved IT security with defined boundaries run into direct conflict with these expectations.

There are more intersections between culture and technology involved here. Individuals have been shown to be more likely to act out through technology given the apparent anonymity such technology provides. Employees also appear less likely to correlate their actions with real, tangible consequences. Accountability for action and clear understanding of consequence are two of the strongest deterrents to action for potential insiders.[14]

Employees also often lack an appropriate sense of ethics while using this new IT/network space. While all levels of the education system provide ethics training for the physical and social contexts where employees interact, not everyone chooses to or understands how to apply these rules in a virtual, technological space. Education needs to address appropriate, ethical behavior and obligations for an individual granted trust and access to a networked IT system.

---

[11] New Web 2.0 and communications technologies present a new class security challenges.

[12] The study found that trust is often poorly understood and many companies grant trust through contracts, partnerships, or supply chains without verification or monitoring.

[13] The terms *attack surface and threat space* used here refer to the number of system vulnerabilities that could be exploited and number of potential attackers and attack tools that might be used.

[14] CERT/CC researcher, Dawn Cappelli, explained that most known IT saboteurs sought anonymity in their sabotage actions and admitted, when interviewed, that they did not expect to get caught. Many were also oblivious to the consequences of their actions both for their employer and for themselves upon getting caught.

Another problem is that IT threat tools, such as viruses, rootkits, and logic bombs are becoming more commonly available and accessible, as well as easier and less technical to apply at a relatively low cost to the user. This trend is increasing the number of individuals who have the ability and capability to launch these sophisticated and dangerous tools on a network, reaching more highly-trusted positions and potential insiders.

As technology has become more portable, so have the tools available to the malicious insider. Malicious code or hacking tools can be accessed via networks or brought into the environment on miniaturized computing or storage devices. Exploit tools such as Trojans and rootkits are increasingly stealthy, which elevates the difficulty of detection and remediation. Future use of emerging technologies such as virtualization will continue to magnify this problem.

Currently, technology implementation options for mitigating insider threats are impractical for most CIKR operators due to the lack of technology maturity and prohibitive cost. These tools are not only expensive to purchase, but also to implement. The first-generation of monitoring and access tools can track network user activity and behavior. Companies with these technologies and supporting policies in place can monitor the activities of their employees on their network systems, but these tools produce a very large amount of raw information that needs to be constantly watched and interpreted. Monitoring and interpreting this information is a large and costly task, and for this reason, use of these tools is not widespread. CIKR operators looking to monitor networks for abnormal behavior and IP theft say they need more sophisticated ways to sort through raw data on network usage. Technology used to mitigate insider threats needs to be able to adapt to the emerging threat tools, which are growing at a faster rate than are the tools designed to address them.

Another important consideration is that monitoring tools are likely to have legal implications, such as personal privacy laws. Companies operating in multiple countries will need to comply with different sets of privacy laws in different countries, which further complicate technology implementations of this type.

C. Globalization

In his request, Secretary Chertoff also asked the NIAC to analyze the potential impact of globalization on the critical infrastructure marketplace. In response, the NIAC found that globalization has introduced enormous macroeconomic forces to the marketplace, forces that are pushing large-scale changes and introducing new threats for critical infrastructure operators.

Globalization is a dynamic to the insider threat, much like the escalating technology and network threats, but it affects each sector differently. Combined, these three dynamics pose serious challenges to companies seeking to address the potential for serious insider threats.

As infrastructure operators adapt to the opportunities of the global marketplace, their corporate boundaries are becoming more global and far more difficult to manage, particularly with respect to ever-expanding IT networks. In addition, the group of trusted insiders within a company's IT and network boundaries continues to expand to include new and distributed groups of employees overseas, where the company may face distinctly different network and IT threats. Further, when these companies operate overseas, they depend upon the countries in which they operate for sensitive and vital infrastructure services like telecommunications.

In these new global areas of operation, companies face new challenges and risks. Globalization has expanded inside access and knowledge of critical infrastructures to new populations that are less verifiable than existing workers. Because critical infrastructure operators are less able to screen individuals in these new populations they may be exposing themselves to greater insider threat risk. The risk involved in developing new workforces without established, reliable methods for employee assessment is unknown. Companies operating in new countries face potential for conflict between cultural or national allegiances and corporate values or priorities. Further, globalization is creating a more nationality-heterogeneous workforce, with more potential political sensitivities and concerns for infrastructure operators.

Multinational corporations face legal obstacles in deterring insider threats, as well. The legal infrastructure to deter insider betrayal is not equally present in all countries. Intellectual Property protections vary from country to country, and enforcement of intellectual property laws varies even further.

Corporate policy directed at insider threats can also face globalization challenges. Cultural norms and legal protections for personal privacy on IT systems vary significantly between countries. For some operators, this has already complicated the process of implementing needed physical and logical security integration.

Finally, the global supply chain used by infrastructure operators has increased the potential for expanded insider threats through "agents" – that is, someone or *something* acting on the behalf of another to gain access or knowledge. For example, many corporations contract to have their software code written in foreign countries. This practice carries the potential that malicious code could be inserted into a company's systems and then later exploited. Corporate decisions for sourcing components of critical systems need careful consideration of the risks involved, and need greater understanding of both existing and emerging threats.

D. Obstacles to Addressing the Insider Threat

During Phase I of the Study, the group deliberated on its investigations and identified the following set of obstacles to addressing the insider threat, as requested by Secretary Chertoff in the January 16, 2007 Study initiation letter to the NIAC. The obstacles highlighted here are tied to the findings outlined in the definition, scope, and dynamics sections.

Lack of Information Sharing

There is not enough information sharing and relevant information/data available on insider "threats" for informed corporate risk assessments and mitigation programs. As a result, the problem is difficult to define. The primary reason for this lack of information is that private sector operators have no "trusted entity" they can call to share information on insider incidents.

Furthermore, there is little incentive for CIKR operators to share information on insider incidents. Sharing can be a vulnerability and can create a competitive disadvantage in the marketplace. Private sector operators seeking information on the insider threat also are reluctant because they see little value in many of the end products resulting from studies.

Despite efforts such as the DHS Protected Critical Infrastructure Information (PCII) program, the majority of the private sector does not view government as a viable third-party information collector. The private sector continues to hold serious concerns about government's protection,

retention, and use of private sector operator information. Legal issues surrounding the Freedom of Information Act (FOIA) and state sunshine laws further complicate efforts to encourage the private sector to share insider threat-related information with government agencies.

Needed Research on Insider Threats

The insider threat to critical infrastructures needs research in the areas of threat identification and threat mitigation. Technology trends not only pose some of the greatest risks, but also offer the greatest opportunities for mitigation tools to address emerging threats. In addition, the CIKR trend toward increasing globalization of business processes needs research on the poorly understood personnel, intellectual property, and network risks. Operators need better tools for identifying personnel risks when screening potential employees. Although there is lots of public debate on the relevance of criminal history records in employment suitability decisions, there is little solid evidence upon which to base these decisions.

Needed Education and Awareness

The current level of critical infrastructure owner-operator understanding and awareness of the insider threat is uneven, and in many cases inadequate. Education and awareness is needed to, not only generate necessary security investment by owner-operators, but to create awareness and vigilance among entire CI-sector workforces. Education and awareness programs will be a key component to generating the organizational shift needed to change the cultural obstacles that exist to insider threat mitigation.

In some sectors, there is significant institutional inertia to corporate culture of an unquestioned trust for long-time employees. Successful insider threat mitigation will require persistent vigilance on the part of executives, management, and workers alike. None of these three groups is likely to welcome this concept, because there are a number of institutional forces at play that will likely increase resistance to insider threat programs. These institutional forces include:

1) unquestioned and unverified trust of employees, after granting employment, especially for long-time employees;
2) poor operator-workforce union relationships;
3) employee expectations of rights and privileges versus obligations;
4) inadequate computer and network ethics education and training;
5) prevailing attitudes about management involvement in workers' personal lives;
6) suspicion for anything that looks like 'big brother is watching'-type monitoring programs; and
7) attitudes about corporate sensitivity of CIKR information.

While most companies acknowledge the need to protect against insider threat, not all operators have structured programs to manage the insider threat risk. Many of the programs that do exist avoid on-going risk assessments of employees in key positions with access to critical operations and/or information.

Education of infrastructure owner-operators about the risks from insider threats is possible. That said, the greater cultural change needed to address the problem and fund solutions will be far more difficult to achieve.

When communicating the threat, government should also consider the need to provide economically scalable solutions or Federal assistance to help protect infrastructure vulnerable assets where owner-operators lack the revenue to implement more costly solutions.

Managing and Maintaining Employee Identification

Identity Management is the process of identifying all employees and maintaining identification and accountability for all actions in the workplace and on company networks. It has become increasingly difficult for operators, particularly those with global operations to perform effective identity management. Policies and protocols for IT system access, physical access systems, and background investigations are needed to ensure proper identification of employees granted access to company facilities and resources. Identification is critical to managing insider threats with proper accountability and deterrence for potentially malicious actions. Companies need to manage the identities of their employees, for entry, access, and accountability. Further complicating this issue is a rise in business outsourcing, which is resulting in *federated identity management*, the practice of relying on trust established by business partners.

Establishing identity through background screening processes is also an obstacle for many operators, as they often lack access to the tools to properly establish that applicants are who they represent themselves to be.

Uneven Background Screening Practices

Similar to the set of assumptions provided to the Study by the Homeland Security Secretary in the Study initiation letter, the NIAC identified that uneven employee screening practices are an obstacle to improved critical infrastructure insider threat mitigation. Employee background screening is not accepted universally across the critical infrastructure sectors, despite its obvious utility. Moreover, sectors have varying levels of access to tools and information to conduct adequate background screens of potential employees. Many operators who screen employees are limited to screens at the initial time of employment and may only have access to state police criminal checks. To mitigate risk, employers need the ability to request national-level criminal background checks and terrorism watch lists screening. Critical infrastructure owner-operators need standard methods and mechanisms to screen against all possible threats and risks.

While the initial background investigation process does help to identify high-risk individuals with a criminal history, allowing employers to make well-informed hiring decisions, these initial investigations will do little to identify existing employees whose behavior changes over time, moving towards insider betrayal. Many cases of insider betrayal come from individuals who were longtime employees. Most operators do not have sufficient programs to monitor behavior of employees in key positions or identify and investigate potential problems. Effective mitigation of these risks requires employers to implement programs that will help to identify and mitigate potential problems before a catastrophic betrayal. Solutions could include periodic re-investigation, behavioral observation, employee morale, and employee assistance programs. Critical infrastructure owner-operators will need best practices tools and policies, for implementing solutions, and in some cases, a significant cultural shift to implement these strategies effectively.

CIKR operators working in multinational environments face larger obstacles in conducting background investigations in foreign countries. These operators need consistent, standardized

methods to make accurate risk assessments for employees in international environments and methods of improving the reliability of available background investigation tools in each location.

The topic of CIKR background screening was explored during the Phase II portion of the Study and is covered in detail in the following *Employee Screening* section of the report.

Technology Challenges

The technology systems that manage physical and cyber security are often "silo-ed" and not interoperable, while insider incidents carry increasing potential for combined physical and cyber techniques to perpetrate sabotage, fraud, and theft. This lack of converged physical and cyber systems slows down the recognition and incident handling of these coordinated, combined attacks. Technology tools for managing insider threats/risks exist, but are prohibitively expensive to implement.

The virtual world is a new space and ethical boundaries are not always clear. As discussed in the findings, computer-based sabotage can be more difficult for CIKR operators to address for two reasons. First, because actions take place on a computer system and lack immediate, confrontational and tangible consequences for the actor, they can be perceived as less real, making the actor feel less culpable. Second, virtual actions can possess a certain level of deniability. Actors can seek and possibly attain anonymity for their actions and avoid being held accountable.

Globalization forces, combining with accelerating technology trends are creating an environment for both domestic and globalized critical infrastructure companies where boundaries and perimeters are effectively diminishing. Networks are increasingly globalized and distributed. Workspaces are trending toward virtualization and portability. These trends are significant challenges to the traditional boundary driven security approach used by most companies today. To protect critical infrastructure service delivery from malicious insider threat behavior, CIKR operators must have access to tools that can help them identify insiders, manage the identity and accountability of all those granted access to their systems, and resilient tools that will protect a company's most sensitive information and assets, independent of actor or data/system location.

Cultural and Organizational Obstacles

Frequently, there are cultural, institutional, and organizational obstacles that hinder the ability of owners and operators to address the insider threat effectively. These obstacles include the often-isolated relationship among IT, security, human resources, and the critical asset owners within a company. Converged IT/security management is critical to addressing insider threats. Corporations and companies frequently look at information security as an IT department problem, but too often, these IT departments lack the perspective to assess the risk of critical assets and lack the resources and funding to implement proper security and risk mitigation strategies.

Long-standing corporate culture is another organizational obstacle that owners and operators must tackle if they are to address the insider threat seriously. Many corporations have institutional momentum for ideas that could slow or even inhibit proper programs to address the existing and emerging dynamics of the insider threat. One example is the tendency to hold

unquestioned trust for existing employees, while vigorously questioning incoming employees. Yet, most insider threats arise from longtime employees.[15]

The simplest, most direct finding on organizational obstacles was that supervisor training presents a significant opportunity for insider threat prevention. Most current supervisor training programs do not address insider threats, such as how to identify employees who are moving down the critical pathway towards betrayal, and also how to create a work environment that lowers aggravating factors and mitigates problems before they manifest. Operators would also benefit from supervisors who are trained on how to properly address an emerging event, and minimize losses once a betrayal has occurred. Such a program needs to be integrated into the CIKR operator's broader insider threat approach, and requires leadership and ownership within an organization to be effective.

[15] Evidenced by the findings presented in the CERT/CC – U.S. Secret Service *Insider Threat Study - Computer System Sabotage in Critical Infrastructure Sectors,* May 2005.

VII. PHASE II – FINDINGS

After developing the Phase I Study findings, which defined the insider threat to critical infrastructures, and explored its scope and dynamics, and the effect of globalization, the NIAC commenced a second phase investigation into opportunities to improve employee-screening processes to better prevent the potential for a catastrophic critical infrastructure insider event. The NIAC's findings and recommendations follow.

A. Employee Screening

The January 16, 2007 Study initiation letter asked the NIAC to investigate potential policy solutions to help CIKR operators to improve their employee screening processes. The Secretary's letter correctly noted that many critical infrastructure operators face significant challenges in screening employees and need appropriate tools and a clear legal environment in which to make these decisions. The letter highlighted three tasks to improve CIKR employee background screens. The first two tasks were "to identify issues, potential problems, and consequences associated with screening employees" and "to identify legal, policy, and procedural aspects of the screening employees, as well as potential obstacles from the perspective of the owners and operators." The final task asked the NIAC to develop policy recommendations from these findings to improve critical infrastructure employee screens. The Secretary challenged the NIAC to construct these measures while being careful to balance the rights of all Americans with the requirements of protecting the homeland.

Initial Findings, Conclusions, and Approach

Phase I explorations had shown the NIAC that employee suitability screens are a critical component of any insider threat risk mitigation program, both at the initial time of employment and also as part of a periodic re-evaluation process. Background investigation checks are used as a tool to verify the accuracy of the information presented by an employment candidate and assess the level of risk present, and as such, background screens are crucial to determining the appropriate level of trust.

Critical infrastructure operators depend upon the ability to place appropriate trust in their employees. Government and the public depend upon CIKR operators to place this trust carefully as well. CIKR owners and operators not only provide the services and goods required to maintain public health, public welfare and economic activity, but they also provide these services to each other. The failure of a single provider has the potential to cause cross-sector or geographically cascading infrastructure failures. These potential cascading failures carry consequences far more serious than the simple failure of a single provider. CIKR operators are investing heavily to protect their operations against external threats that could cause such a failure, but a hostile insider with access to vulnerable critical systems, potentially combined with knowledge of that system has the potential to cause events that would far exceed the consequences of an intrusion or attack. It is vitally important that government support CIKR operator efforts to reduce these risks through improved employee screening processes. Although background investigations will not eliminate insider risks altogether, application of a thorough, systematic approach to accurate, comprehensive information can significantly mitigate insider threat risks faced by critical infrastructure operators.

The Study examined common suitability screening practices and identified common elements of a quality program. As a risk mitigation tool, background investigations should be structured to identify potential risk indicators in a candidate's background. Effective background screening programs have a written, clearly articulated, and well-communicated process for gathering and evaluating all available information relevant to the position and level of trust.

The investigation process collects, examines, and verifies all information before beginning the adjudication process. Important information sources used in background screenings can include: Federal terrorism information, criminal history records, driving records, and credit records. Also critical to this process is careful scrutiny and verification of information presented in the application and interview process. Good adjudication processes are clearly articulated, consistently applied, and consider the "whole picture" presented by the information about a candidate to determine an appropriate level of trust. This approach helps to establish consistency in employment decision making, which can also help to protect employers from litigation by demonstrating a clear legal basis for decisions that could be called into question. Adverse information is appropriately weighted for job relevance and risk posed by the level of trust required for the position, and discussed with the candidate to determine potential mitigating circumstances.

Given the current threat environment, the NIAC found that CIKR screening programs should include measures to address the risk posed by potential terrorist organization infiltration or employee recruitment. To do this, CIKR operators will need access to Federal terrorism screening programs. DHS is currently developing a program to enable the screening of certain private sector employees and employment candidates through the Terrorism Screening Data Base (TSDB). This process will help to mitigate terrorism risk for CIKR operators, but will not entirely prevent it, and therefore must be part of a comprehensive program.

Based on the Study initiation letter from Secretary Chertoff, preliminary discussions identified that the clearest opportunity to improve CIKR employee screens was through access to criminal history records. The majority of the Phase II investigation focused on developing recommendations to improve the availability, accuracy, and value of criminal history information for CIKR operator employee screens. These investigations not only explored how government could go about improving CIKR operator access to this information, but also considered its value, sensitivity, and appropriate use in background investigation screens.

Current Statutory and Resource Environment for CIKR Criminal History Background Checks

To address the challenges posed to the NIAC by Secretary Chertoff in the initiation letter, the NIAC carefully investigated the current laws, structures, and mechanisms available for using government criminal history records in CIKR employee screening. The recently written, *Attorney General's Report on Criminal History Background Checks* was the starting point for much of the NIAC's findings on the challenges involved in improving CIKR criminal history background checks.[16] The Attorney General's Report, submitted to Congress in June 2006, is a

[16] See *The Attorney General's Report on Criminal History Background Checks (June 2006)*, available at www.usdoj.gov/olp/ag_bgchecks_report.pdf. See also, "Employer Access to Criminal Background Checks: The Need for Efficiency and Accuracy," Hearing Before the Subcommittee on Crime, Terrorism, and Homeland Security of the Committee of the Judiciary, House of Representatives, 110th Cong. (April 26, 2007) (Prepared Statement of

clearly presented 148-page comprehensive examination of the issues and laws involved in the potential for private sector use of government criminal history records. The report was developed in response to a provision of the Intelligence Reform and Terrorism Prevention Act of 2004, which reflected Congress's interest in developing a more considered and simplified system for employer access to FBI fingerprint criminal history records. The report helped to inform the NIAC's understanding of the complex issues involved. The Study's findings on the current legal and resource environment for criminal history background checks, which were largely drawn from the detailed background section in the Attorney General's Report, follow.

Private sector interest in using criminal history records for risk assessment in employment decisions has increased significantly in recent years. The National Employment Law Project (NELP) testified to Congress that 80 percent of large U.S. employers use criminal history records checks today, up from just 50 percent in 1996.[17] Some regulated industries, such as the Nuclear, Banking, and Securities Sectors, are granted access to Federal and State criminal history records data through Federal statutes. Other employers subject to state regulation or licensing may submit fingerprints for similar checks, pursuant to a patchwork of state statutes approved by the Attorney General. Most employers, however, lack this legal authority for access to fingerprint checks and, therefore, typically turn to third-party professional background screening and data companies to run name checks on employment candidates and verify the accuracy of records obtained.

Within those sectors and industries that have statutory access to Federal government criminal history records, companies are able to submit candidate fingerprints, typically through a State Identification Bureau, to the FBI's Criminal Justice Information Services (CJIS) Division to check for records against the national criminal history record index, the Interstate Identification Index (III). The III, or "triple-I", is a segment of the Integrated Automated Fingerprint Identification System (IAFIS), which uses fingerprints to assure positive identification of offenders, helping to avoid false-positive record association and false negative "no record" responses, which is possible with name-only checks of less comprehensive criminal history databases.[18] The III is part of the National Crime Information Center (NCIC) records, and includes information submitted to the FBI by all fifty states and five territories, as well as county courthouses and police agencies across the country.

One problem with the use of III records for background checks is that the system was designed for the use of criminal justice officers, and not for non-criminal justice records checks. While the III can provide a multi-state view of an offender's *rap sheet*, [19] it often misses records available at the State-level, particularly those relating to non-serious offenses, and it can include information previously purged from a State record as a part of an administrative or adjudicative process. Most significantly, the III is missing dispositions on roughly half of the arrest records it

---

Frank A.S. Campbell, Senior Counsel, Office of Legal Policy, United States Department of Justice, summarizing the Attorney General's Report and its recommendations).

[17] Id. (Prepared Statement of Maurice Emsellem, Policy Director, National Employment Law Project, p. 2).

[18] *The Attorney General's Report on Criminal History Background Checks*, page 14.

[19] A Rap sheet stands for Record of Arrest and Prosecution, (*from the AG Report, page 14*). While arrest records alone are often not usable in employment decisions, these records do provide the advantage of informing screeners of an arrest cycle and tells them where they can find the complete record, improving understanding of risk with a candidate. In addition, arrest records can be considered under certain circumstances in employment screening consistent with EEOC Guidelines.

contains. In these cases, the database cannot identify whether the arrests resulted in a conviction, acquittal, dismissal, or otherwise.[20] The missing dispositions for these arrest records are the cause for much of the concern with privacy and fair use advocates involved in the debate.[21] Nevertheless, The Federal criminal history records contained in the III are viewed as the most comprehensive U.S. criminal history records available.

Not surprisingly, State-level statutes for access to criminal history records vary significantly from state to state, as do the quality and use of the records contained in state criminal history databases. State records can include IAFIS fingerprint records as well as name-only records, and a portion of every State's records are not indexed at the Federal level. For example, Florida has one million records that are not included in the FBI database and only 30 percent of Florida's warrants are in the Federal system.[22] These records are not entered into the III for a number of reasons, including failure to meet III standards for inclusion (missing or improper fingerprints, for example), but also because states often lack the resources to maintain the accuracy of Federal records. For these reasons, state records repositories are more inclusive and more complete than Federal, but still only have dispositions on seventy to 80 percent of the arrest records they contain.[23]

Critical infrastructure employers who lack statutory access to Federal or State criminal history records turn to private screening companies when they need to conduct criminal background checks on prospective employees. These companies include a variety of different businesses, from professional background screening companies to large consumer data companies that run large multi-state criminal history databases. These consumer data companies and professional background screening companies are regulated by the Fair Credit Reporting Act (FCRA) and are commonly referred to as Consumer Reporting Agencies (CRAs).[24]

Multi-State databases, which are operated by companies such as *Lexis-Nexis*, *ChoicePoint*, and *Background Screening of America*, are aggregations of public records available through county courthouses and other sources from all across the country. These databases are not geographically comprehensive in their coverage, and do not include data from all States or even all counties within the States they cover. Multi-State databases offer companies some level of assurance that they will find undisclosed adverse criminal history information on a prospective employee, but are the least reliable of the potential data sources. Multi-State databases are limited to name-only records, and by design, are periodically out of date for different sources.[25] Many employers who access records through these multi-state databases, as well as some who access Federal and State records, follow-up each criminal record entry through a contracted

[20] According to the Bureau of Justice Statistics, approximately 70 to 80 percent of state-held arrest records have final dispositions, as compared to the approximately 45 to 50 percent of FBI-maintained arrest records with final dispositions - from the *Attorney General's report on Criminal History Background Checks*, April 2006, page 18.
[21] Add a discussion here on how many arrests result in felony convictions.
[22] From discussions with Donna Uzzell, Director, Criminal Justice Information Services, Florida Department of Law Enforcement and Chairman of the National Crime Prevention and Compact Council, November 15, 2007.
[23] Recent arrest records have a higher rate of disposition information, *The Attorney General's report on Criminal History Background Checks*, April 2006, pp 18, 27.
[24] The role of the FCRA in regulating use of criminal history information is discussed in detail on pages 43-45 of the Attorney General's Report on Criminal History Background Checks.
[25] *The Attorney General's report on Criminal History Background Checks*, April 2006, p 38.

professional background screening company that checks each record at the courthouse where it originated.

As an alternative to multi-State database record checks, some professional background screening companies check court records for all counties disclosed as a residence by a candidate. They also run a credit report that identifies all past residences for an individual, allowing them to check records in those jurisdictions as well.

In sum, all of the criminal history information sources are incomplete or inaccurate to different degrees and in different ways. The challenge is to develop a system that efficiently provides the best and most accurate information possible.

Federal and State Laws on Access

Currently, there are several different Federal laws that grant different industries access to Federal criminal history records for background checks. Historically, most criminal background checks of FBI criminal history records for non-criminal justice purposes have been done under the authority of Public Law 92-544,[26] which was passed in 1972 and provides access to Federal criminal history records to State agencies for licensing and employment checks.[27] To access these Federal records, the State must have passed a specific statute under PL 92-544 to authorize FBI fingerprint checks for licensing and employment in the industry or sector.[28] There are approximately 1,200 State statutes enacted under PL 92-544.[29] The results of these checks are passed to a designated State or local government agency, which is responsible for screening candidates based on agency or statutorily-identified criteria.

There are exceptions to the P.L. 92-544 state statute-based approach. Federal laws provide specific private sector employers access to criminal history records in selected industries. For example, The Volunteers for Children Act (VCA), an amendment to the National Child Protection Act (NCPA) of 1993, allows record checks of individuals working or volunteering with children or the elderly without a requisite P.L. 92-544 State statute. However, State agencies must screen check results against pre-set criteria for employment suitability. As noted in the *Attorney General's Report on Criminal History Background Checks*, this did not achieve the intended effect of broadening access through State background check programs because many States either lacked the resources to do so or, as a policy matter, did not want to have state agencies perform employment or volunteer suitability screening for private qualified entities.[30]

Congress also passed a law to improve State cooperation in sharing criminal history for non-criminal justice purposes. The National Crime Prevention and Privacy Compact (Pub. L. 105-251) of 1998 establishes a legal structure governing the exchange and use criminal history information for non-criminal justice purposes. The Compact is intended to clear up confusion about sharing records between States and set the rules of the receiving state as the standard for use. Rules implementing the provisions of the Compact are promulgated by the Compact Council, which is a governing body made up of Federal Agency and state representatives

[26] This trend has changed somewhat recently with the addition of the port workers screening programs and Transportation Workers Identification Card (TWIC) program, among others.
[27] *The Attorney General's Report on Criminal History Background Checks*, April 2006, p. 19.
[28] *The Attorney General's Report on Criminal History Background Checks*, April 2006, p. 19.
[29] *The Attorney General's Report on Criminal History Background Checks*, April 2006, p. 19.
[30] *The Attorney General's report on Criminal History Background Checks*, April 2006, page 21.

appointed by the Attorney General. The Compact Council also provides a means for State input into non-criminal justice use of criminal history records in the III. Primary among the Compact rules is the finger print requirement, which provides for improved positive identification.

Currently, 28 states have ratified the Compact, and several others have committed to follow the rules established by the Compact Council. The Compact does not provide any additional authority for employers to access criminal history records. The Compact and the rules promulgated under it govern how III information is shared for non-criminal justice purposes and establish the procedures for access and use. For example, the Compact Council has issued a rule allowing authorized non-criminal justice users of III information to outsource non-criminal justice administrative functions in connection with the use, such as the collection and submission of fingerprints, obtaining missing dispositions, and making fitness determinations. New or expanded authority for non-criminal justice access, however, must be established through Federal or State statutes.[31]

Recent Congressional efforts to expand access to Federal criminal history records information nationwide for different industries have fallen short due to the continued reliance in the law on having state agencies serve as the suitability reviewers in the background check process. The Private Security Officer Employment Authorization Act (PSOEAA), part of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, authorized private security company employers to submit fingerprints to State Identification Bureaus that, in turn, are authorized to conduct criminal background checks on employment candidates using a Federal fingerprint check.[32] The results are to be returned to a State agency, which is to apply either existing State criteria for the suitability of private security officers or the default Federal criteria set forth in the PSOEAA. Again, largely due to resource constraints, many States that do not otherwise have a State licensing program for private security officers have opted not to establish a program for such state-adjudicated background checks under the PSOEAA. The result is that security companies in these states have still been unable to obtain fingerprint-based background checks of FBI data for screens on their employees under the federal statute.[33]

As noted earlier, some regulated critical infrastructure sectors and industries do have statutory access to review Federal criminal history records. These include federally chartered or insured banking institutions, the nuclear sector, nursing homes, and the securities industry. Other recent laws have added regulatory requirements for screening certain airport employees, applicants for hazardous materials endorsements to state issued commercial drivers licenses, and port workers through a Federal regulatory agency process.[34] However, for the rest of the critical infrastructure sectors, access to Federal and State criminal history records is uneven and varies widely from state to state.

---

[31] See Security and Management Control Outsourcing Standard, National Crime Prevention and Privacy Compact, Notice, 70 Fed. Reg. 74373 (Dec. 15, 2005).

[32] The PSOEAA was part of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004.

[33] See "H.R. 2703, Private Security Officer Employment Authorization Act of 2007," Hearing Before the Subcommittee on Health, Employment, Labor, and Pensions, Committee on Education and Labor, House of Representatives (February 26, 2008) (Prepared Statements of Frank A. S. Campbell, Senior Counsel, Office of Legal Policy, United States Department of Justice, and Donna Uzzell, Director, Criminal Justice Information Services, Florida Department of Law Enforcement and Chairman of the National Crime Prevention and Privacy Compact Council).

[34] Attorney General's Report on Criminal History Background Checks, June 2006, page 20.

Restrictions on the Use of Criminal History Records in Hiring Decisions

A multitude of Federal and State laws govern the use and privacy protection of the public criminal history records compiled, collected, and utilized by CRAs in industries that lack statutory access to government criminal history records. The Fair Credit Reporting Act (FCRA) of 1970 regulates third-party CRA companies that some critical infrastructure employers use to screen their employees. The FCRA governs the use of criminal history information by consumer reporting agencies at a Federal level, providing a minimum standard of individual privacy protection. The FCRA is also intertwined with the State Consumer Reporting Agency laws present in roughly half the states, some of which are more restrictive than the FCRA. The FCRA includes safeguards for protection of individual privacy, allowing for criminal history information on an individual to be shared only when an employer is making a suitability determination. The FCRA also includes measures to assure information accuracy and a requirement to provide notice to candidates when a search will disclose adverse information to an employer.

In addition to the FCRA and State CRA laws, other Federal and State laws that prohibit employment discrimination are also applicable to the criminal history background process. Title VII of the Civil Rights Act of 1964 prohibits employment discrimination based upon race, color, religion, sex, or national origin and provides monetary damages for cases of intentional employment discrimination. The Equal Employment Opportunity Commission (EEOC) enforces these laws, and the commission has provided guidance to employers on the relevance of convictions in hiring decisions. The EEOC outlined three factors to consider, which include: the nature of the crime for which the individual was convicted, the time passed since the conviction, and the nature of the job held or sought. The EEOC further clarified that lifetime disqualification from a position should be applied only in special circumstances relating to the nature of the position, the nature of the offense, or both. The EEOC has also issued guidance to employers on how arrests that have not resulted in a conviction should be considered in employment decisions, requiring additional inquiry about the arrest context and an opportunity for the applicant to explain. Some States have also passed Equal Employment Opportunity laws that regulate the use of this information. These laws range from prohibiting employment discrimination against people with criminal records to prohibiting the use or inquiry of arrest records and certain types of convictions. Currently, 11 States have laws that govern and prohibit use of these types of information in hiring decisions.[35]

Recommendations by the Attorney General

The primary conclusion of the Attorney General's Report is that there is need to revisit the authorities under which checks of FBI criminal history can be made for non-criminal justice purposes. The Attorney General's Report also outlines recommended, carefully considered rules and conditions to address fair use, ex-offender reintegration, and privacy protection.

The Attorney General's Report presents a well-considered case for expanding access to Federal criminal history records. To begin, the report notes that criminal history record checks are increasingly common in the private sector through FCRA-regulated companies. The argument follows that if employer risk assessments were going to be based upon criminal history screens, then public interest would be best served if these screens were as accurate as possible. The

[35] See generally, The Attorney General's Report on Criminal History Background Checks, pp 47-50.

Attorney General's Report proposes that government criminal history records will improve the accuracy of these employment suitability screens. The Report does not cast aside concerns of infringement upon personal privacy or fair use of these records. The Attorney General's Report does not advocate change to the Federal and State laws that govern how these records should be protected or applied in screening decisions.

The report's carefully detailed recommendations cover 16 pages and address a wide range of policy and structural issues necessary to building a successful statute for achieving these goals. If enacted, the report's recommendations would provide CIKR operators the access needed to improve critical employment risk assessments. Key aspects of the recommendations that echo the NIAC's concerns include:

- Screened records should be provided directly to employers or their CRAs for suitability determinations.
- Access should be provided through states to improve accuracy, while also establishing a means for doing checks in states that do not participate.
- Includes measures to improve the accuracy of records disseminated and appropriate screening to ensure state and federal laws limiting access and use of criminal records are not violated.
- Includes privacy and fair information practice requirements, based upon the protections in the FCRA, including: user enrollment, use limitations, Privacy Act-compliant consent and notice, rights of review and challenge, a streamlined and automated appeal process, limits on user re-dissemination, information security procedures, compliance audits, and statutory rules on the use, retention, and destruction of fingerprint submissions.
- Access for private sector background screening companies, as subject to the Fair Credit Reporting Act (FCRA) and applicable consumer reporting laws.[36]

The report also suggested that authorization should consider providing guidance to employers on suitability criteria to be used in criminal records screening, an issue important to the NIAC.

The Justice Department provided significant assistance to the NIAC during its exploration of this subject and helped to identify and contact key stakeholders in the public policy debate around the issue. These groups included privacy rights advocates, ex-offender rehabilitation advocates, state law enforcement and records organizations as well as professional background screeners. After a full investigation of the subject, the NIAC reached a set of conclusions similar to the AG Report. The Study's key findings follow.

More Findings on Employee Screening

The NIAC also deliberated which CIKR employees should undergo a comprehensive screening process. Consistent with previous NIAC studies, this investigation concluded that a one-size-fits-all broad application set of rules or requirements is not appropriate. CIKR sectors are very different and the risks these operators face due to insider or other threats vary greatly. Each operator will have to evaluate the risk posed by different positions within their company and apply their own solution. As guidance to help operators in conducting these assessments, the NIAC concluded that a common starting point for this evaluation process should be an employment position's *access to the vulnerabilities* of a CIKR operator's *security, systems,*

[36] Compiled from the Prepared Statement of Frank A. S. Campbell, Senior Counsel, Office of Legal Policy, United States Department of Justice, supra., n. 1.

services, products, or facilities that could provide the opportunity to cause significant harm. Further, CIKR operators should consider more vigorous, human reliability-type programs with monitoring, and periodic evaluations and re-investigations for positions that, along with access to vulnerable systems, also include operational *knowledge of critical systems* and their vulnerabilities.

One of the most important findings the group uncovered on this topic is that the presence of a criminal history record by itself is not a clear indicator of risk. The NIAC found a consensus among experts that for some more serious types of convictions, a broadly applicable risk is always present. However, for other types of convictions, research on recidivism indicates that risk diminishes with age and time. Currently, there is no research available that directly correlates criminal conviction history with employee risk. In contrast to government screening programs that apply "bright-line" criteria as a lone determinant for suitability, many CIKR operators use criminal history information as a part of the picture when looking for patterns that indicate risk. Employers can most readily identify these significant risk factors, such as a history of boundary pushing and rule-breaking behavior, chronic substance abuse, and pathological anti-social behavior through review of criminal history records.

The fingerprint component of Federal III checks was found to be the most valuable and compelling aspect of government criminal history records. Federal and most State criminal history records are fingerprint-based records, which ensures positive identification. Private sector records checks are name-based and name based records checks carry the potential that a candidate with a criminal history could be living under an assumed name or stolen identity. Analysis of FBI records checks has shown this to be a significant risk. In 1997, roughly six-hundred-thousand of the FBI's fingerprint checks conducted for employment and licensing purposes produced criminal record 'hits', and 11.7% of individuals screened for those hits provided names that were different than what was listed on their criminal history record. These records would have been missed by a name-only check.[37] For employers, positive identification is more that whether or not a criminal history record gets by them – positive identification and full disclosure is an important part of establishing a trust relationship with an employee. Employers say this type of full-disclosure trust cannot happen if an employee withholds requested information and is constantly worried that this will be discovered. This magnifies an operator's potential risk. Fingerprint records have the potential to strengthen the trust relationship between employer and employee, even in the presence of a criminal record.

One topic the NIAC explored extensively was the issue of privacy rights. The Study learned that while criminal history records are public to the extent that they are available through courthouses and private-sector CRA companies, these records do rise to the level of what the government considers privacy-protected information. The concept of *privacy* can be described as the expectation that an individual can maintain a personal space, free from interference by other people or organizations.[38] Privacy information extends to any personal information about and individual collected and attributable to them. For criminal history records, privacy information is more than the data on an individual's RAP sheet; it includes any information that could be inferred from it or even that a record exists. Criminal history records are very sensitive as privacy information and have the potential to excessively harm the welfare of an individual as a

[37] From the AG report, p. 26.
[38] Roger Clarke, "What is Privacy?" August, 2006. http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html

result of negligence or misuse. Any program implemented to expand the use of government criminal history records must include provisions to protect the privacy rights of all Americans.

The NIAC worked with privacy advocates and experts to identify what measures would be necessary to ensure an individual's right to adequate privacy protection. As a result of these discussions, the NIAC found that an implemented program would need to include: the rights of and individual to know and consent to a records check; the right of an individual to review, challenge, and correct inaccurate information on their record; and the right of an individual to appeal a decision based upon inaccurate information. Privacy protection requirements for information users should include: user enrollment agreements; standards for privacy information handling and protection; limitations on use and dissemination of information; criminal penalties for negligent or miss-use of information; and user program compliance audits.

The NIAC also found reason to include consideration for ex-offender reintegration in its recommendations. Ex-offender reintegration is the body of public policy that concerns how government should seek to reintegrate criminal offenders as productive and law-abiding members of society. The NIAC's recommendations have the potential to significantly affect business and hiring practices nation-wide. Calling for stronger background investigations for CIKR workers could have the unintended effect of prompting employers to screen all employees and uniformly exclude individuals with conviction or arrest records. This outcome would be counter-productive to the goals of the Study and could result in the creation of a very large class of disaffected, unemployable Americans. The NIAC acknowledges that its screening program recommendations significantly affect these other areas of public policy, which need to be considered carefully in any implementation. Screening program recommendations need to include measures to minimize the effect on ex-offender reintegration as well as provide direct incentives to encourage employers to consider risk-appropriate hiring for ex-offenders.

Addressing the Assigned Tasks

In his January 16, 2007 letter to the NIAC, Secretary Chertoff asked the Council to address two sets of issues. First, he asked the NIAC to *identify issues, potential problems, and consequences associated with screening employees.* Second, the Secretary requested the NIAC to *identify legal, policy, and procedural aspects of the issue, as well as any potential obstacles, from the perspective of the owners and operators.* The NIAC's response to these two tasks follows.

Issues, Potential Problems, and Consequences

In enacting a legislative solution, policy makers and legislators should consider its implications on other policy and government institutions and attempt to anticipate unintended consequences. The NIAC engaged in this process in developing its recommendations on screening policy. In his letter that initiated the Study, the Homeland Security Secretary asked the NIAC to consider *issues, potential problems, and consequences associated with employee screening programs.* The NIAC identified the following:

1. Expanding the use of FBI RAP sheets for use in employment risk assessments by private sector employers also expands the potential for personal privacy violations, which is a fundamental concern for all Americans. The highest privacy protection measures are crucial to any program established to expand access to this information for private employment screening purposes.

2. Expanded program access to criminal history records could have the unwanted effect of making it more difficult, or impossible, for, the significant number of Americans with criminal histories to obtain gainful employment and meaningful reintegration into society.
3. RAP sheets contained in the Federal III and State records were not designed for non-criminal justice use. As a result, they are difficult to read and often missing dispositions on arrest records, which makes them poorly suited for accurate screening purposes.
4. The current method of Federal or State agency record adjudication that is used under P.L. 92-544 will not work for a CIKR screening program many reasons, the most limiting being the resources required to meet the unprecedented volume and complexity of this task.
5. Federal and State criminal records systems and organizations lack funding, resources and capacity to support a significant increase in non-criminal justice use of their systems.

Legal, Policy, and Procedural Issues and Obstacles

The Secretary also asked the NIAC to *identify legal, policy, and procedural aspects of the issue, as well as any potential obstacles, from the perspective of the owners and operators.*

The NIAC identified the following *legal* issues faced by CIKR companies in establishing effective background investigation processes:

1. CIKR companies need statutory authority to access records
2. Programs implemented need to fit within the existing legal framework of State and Federal Fair Credit Reporting (FCR) and Equal Employment Opportunity (EEO) laws

The NIAC identified the following *policy* issues faced by CIKR operators in establishing effective background investigation processes:

1. Need for a critical infrastructure-focused near-term solution
2. Solutions need appropriate funding to support increased records use and CIKR operator support from both Federal and State records bureaus
3. Solutions need to encourage, fund, or provide incentives for State participation optimize records accuracy and presentation
4. Solutions need to include programmatic measures to improve records completeness, accuracy, and presentation[39]
5. Need for research on the nexus between criminal history and insider threat employee behavior to improve the value of CH information in screening risk assessments and also to protect individuals from undue discrimination

The NIAC identified the following *procedural* issues faced by CIKR operators in establishing effective background investigation processes:

1. Need to allow operator discretion in choosing when to participate
2. Need to allow operators to directly access criminal history information for screening
3. Need to allow operators to set and apply their own screening criteria

[39] Congress passed the NICS Improvement Act in December 2007, which was subsequently signed by the president in January 2008. This law authorizes significant funding for improvements and updates to criminal history records used for firearms background checks, and if fully funded and implemented will significantly improve the accuracy, completeness, and presentation of federal and state criminal history records.

4. Need to provide for third-party screening company (CRA) involvement in the screening processes

The final task assigned by the Homeland Security Secretary's letter was to develop recommendations to improve critical infrastructure employee screens. The NIAC developed a set of recommendations to address each of the points identified here. These recommendations follow in the recommendations section.

VII. RECOMMENDATIONS

As requested by Secretary Chertoff in the January 16, 2007 letter, the NIAC identified areas that require new policy to improve critical infrastructure protection from insider threats. The following recommendations are the NIAC's carefully considered outcomes from that process.

None of the NIAC's recommendations should be construed as a call for regulation. The Report's recommendations and suggested approaches are intended to focus and optimize CIKR operator resource allocations to achieve elevated insider threat protection. The NIAC found no cases where increased regulation would better achieve this goal.

Information Sharing

The NIAC identified three areas where information sharing would improve understanding of insider threat, risk, and mitigation.

1. To address the critical infrastructure owner-operator need for timely and relevant strategic-level information on insider threats, the NIAC recommends that government establish a mechanism to communicate government intelligence agency understanding on insider threats. To achieve this, government should make use of cleared personnel in each sector and provide periodic, useful briefings on developments about insider threats.

   To address a specific information-sharing obstacle identified by the NIAC between government and critical infrastructure owner-operators, the NIAC recommends that government develop a mechanism and validated process for sharing information on national security investigations, which currently does not exist.

2. To improve owner-operator knowledge of the risk of insider threats, the NIAC recommends that each sector establish a trusted process and mechanism to share incident information on insider threats in a protected manner. Information collected by each sector can then be aggregated and anonymously protected information. This anonymized, protected information will help to develop better understanding of the enterprise-level risks, facilitating more accurate risk assessments and driving appropriate security investment.

   The NIAC has identified that Information Sharing and Analysis Centers (ISACs) in many sectors are well positioned to fulfill this role. Where ISACs are not available, or cannot fulfill this role, Sector Coordinating Councils (SCCs) should investigate options to develop a commonly acceptable solution.

3. To address the need for sustained support to CIKR operators in dealing with insider threats, the NIAC recommends that government coordinate a clearinghouse resource for owner-operators to assist in the process of assessing and mitigating their insider threat risks.

   This clearinghouse should leverage the Education and Awareness recommendation and framework along with the Best Practices framework to assist in developing insider threat mitigation programs as well as operational support in dealing with ongoing insider incidents.

Research

Further, the government should fund research to develop information and understanding about different aspects of the insider threat, which can be used to improve programs and resource allocation by CIKR operators. The NIAC identified the following critically needed areas for study:

1. Research on insider threats in the context of globalization and the effects of outsourcing, global operations, and diversifying work forces.
2. Research the intersection between a history of criminal convictions and employee behavior, including insider threats. This research will not only help to improve risk assessments for CIKR operators, but will also help develop policy to help protect individuals from undue employment discrimination.
3. Research outlined in the technology recommendations section to address challenges emerging due to growing technology threats.

Education and Awareness

The NIAC identified that education and awareness offer the biggest potential return for policy in motivating CIKR operators to focus their efforts to address the insider threat. The NIAC has developed a framework for outreach and awareness along with a framework for best practices and policies, which can assist in developing the programs for implementing a program that will increase education and awareness of insider threats and solutions for corporate leadership in all sectors.

1. The NIAC recommends that leadership for national insider threat programs come from the Executive Office of the President, working through a program to be established at DHS, to coordinate government support CIKR operator education and awareness of insider threats.
2. The NIAC recommends government should establish a program whose goals are to develop a common baseline understanding of the emerging and dynamic insider threat to critical infrastructures. Furthermore, the program should help promote the broad corporate cultural changes needed to elevate internal security and protect against the insider threat. This program should:
    e. Leverage the leadership of the office of the President and the Critical Infrastructure Partnership process to work directly with CIKR executive leaders and communicate the potential enterprise risks involved;
    f. Partner with leading companies in each sector to establish pilot programs that will create the effect of a new industry standard;

g. Educate executives on potential actors and motivations involved in insider threats, potential consequences, and a process executives can employ to identify critical (enterprise-level risk) insider threat-vulnerable positions within their company, as well as potential policy and technology solutions to stimulate needed executive leadership on this issue;
h. Assist CIKR operators in developing education and training programs for managers and employees that elevates the value of internal facing security in corporate culture to better protect against the insider threat;
i. Identify and support future research needed to improve insider threat mitigation programs; and
j. Apply the principles outlined in the attached Outreach and Awareness and Best Practices frameworks to help CIKR operators to develop insider threat programs tailored to their needs.

Technology

To address the technology gaps identified in the findings section, the NIAC has identified four areas of recommended policy action.

1. To improve critical infrastructure owner-operator security posture towards present and emerging insider threat technology challenges, the NIAC recommends that CIKR operators establish as a priority that they maintain current network/IT security best practices.
2. The NIAC recognizes that hardware and software assurance issues exist and are of critical importance to CIKR operators, carrying the potential for massive insider threat consequences. The recent Defense Science Board Report explored this issue. The NIAC recommends that this work be leveraged and the process continued to identify solutions to this significant challenge to CIKR surety.[40]
3. To improve CIKR worker IT/network ethics, accountability, and understanding of appropriate conduct on critical infrastructure IT networks, the NIAC recommends the following actions:
    a. Government leadership on insider threat programs should establish programs to develop secondary education training on ethics and awareness of real consequences of cyber actions for future workers.
    b. Congress and the Justice Department should improve accountability for virtual crimes through improved prosecution and equitable punishment for the tangible consequences of cyber crimes.
    c. Encourage CIKR operators to establish and enforce greater network action accountability with stronger identity management tools, and worker education programs.
4. To address emerging technology obstacles outlined in the findings section, the NIAC recommends government convene a steering group of IT technology experts to explore insider threat technological solutions, using the following areas as guidance:

[40] *Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software,* September 2007.

a. Improved identity management technologies and tools for the purpose of creating a strong, persistent, portable, and platform independent secure network/ physical access identity for CIKR workers.
b. Improved information protection technology applications to assist in protecting CIKR operator sensitive data through development of stronger, persistent, and more useful data protection or *mandatory access control* tools.
c. Improved cross-platform insider threat data correlation tools, to assist CIKR operators with identifying anomalies and insider threat behavior patterns across heterogeneous IT systems and physical access systems.
d. Continued development of network/IT psychometric tools to improve threat identification and understanding.
e. Examine the insider threat problem from a risk management level and develop a systematic IT insider threat mitigation approach to assist both developers and CIKR operators in their processes.
f. Examine emerging trends and develop guidelines for technologies to mitigate insider sabotage through IT systems management, which because of its level of access, carries potential for widespread and disastrous consequences.

Employee Screening

Through its investigations and deliberations, the NIAC has found that CIKR operators need access to fingerprint-based Federal and State criminal history records to improve insider threat risk assessment and increase the surety critical infrastructure services delivery. To achieve this, the NIAC recommends Congress provide CIKR operators with access to these records as a part of a comprehensive program, as outlined in the recommendations of the June 2006 Attorney General's Report. The NIAC recommends this program place particular emphasis and consideration on the needs of CIKR operators, as is outlined in the recommendations below:

1. The Federal government should provide uniform statutory access for CIKR operators to federal fingerprint criminal history records to improve the accuracy of CIKR employee risk assessments.
2. To accommodate the diversity of CIKR operators, the implementation should avoid a one-size-fits-all approach. This program should provide CIKR operators the discretion:
    a. to choose when to participate and screen employees;
    b. to review and assess employment candidate criminal history records directly, subject to state and federal legal restrictions;
    c. to establish their own adjudication criteria to meet differing levels and types of risk;
    d. to use the program to screen current and prospective employees on an as needed basis; and also
    e. provide access to third-party FCRA-regulated background screening companies to allow them to continue to assist CIKR operators in their screening processes.
3. To protect the rights of individual privacy, this program, as the Attorney General's Report recommends, should adhere to the existing FCRA privacy standards for criminal history checks in the private sector. Most importantly, these protections should include:
    b. the rights of an individual to know and consent to a records check;
    c. the right of an individual to review, challenge, and correct inaccurate information on their record; and

d. the right of an individual to appeal a decision based upon inaccurate information.

Privacy protection requirements for information users should include:

a. standards for handling and protecting privacy information;
b. clear limitations on use and dissemination of privacy information;
c. criminal penalties for negligent use or misuse of information;
d. user enrollment agreements, similar to those used with law enforcement organization access; and
e. user program compliance audits.

4. To maximize the accuracy of the information used for employment screening, programs implemented to screen CIKR employees should:
    a. include funding for measures to improve the accuracy of records;
    b. include funding for measures to standardize the presentation of records;
    c. include funding to develop programs to educate users on how to read RAP sheet records; and
    d. be conducted through an agency in the state of employment where possible, and through a federal agency where this option is not available through state laws and programs.
5. Legislation should provide appropriate funding for the Justice Department, State records bureaus, and other involved agencies necessary to achieve a near-term solution for this program. As outlined in the AG Report, the program should transition to a fee-based funding solution over time, so long as fees remain reasonable enough that small operators can participate, and all involved government parties receive an appropriate share.

In addition to the recommendations above, which echo the recommendations of the Attorney General's report, the NIAC also recommends the following measures:

6. To address the broad societal need for ex-offender reintegration, the program should include guidance for employers in the use of criminal history information in employment risk assessment. The program should include measures that provide liability protection for employers who adhere to a national set of fair use guidelines like the TSA screening guidelines or the recently proposed New York State liability protection measure. A national set of fair use guidelines, developed and updated from the best-available research, would allow for employment and re-integration of ex-offenders without increasing risk to our critical infrastructures.
7. To improve the value of the information provided to CIKR operators through this program and also to help develop guidelines that will protect individuals from undue employment discrimination, government should conduct research on the nexus between criminal history and insider risk, as is outlined in the research recommendations. Outcomes from this research should be used to refine the national fair use guidelines described in the recommendation above.
8. The NIAC recommends that Congress and the Justice Department act swiftly on these recommendations to improve public safety and surety of CIKR services delivery soon.

VIII. APPENDICES

APPENDIX A: REFERENCES

Aleman-Meza, B., Burns, P., Eavenson, M., Palaniswami, D., and Sheth, A. "An Ontological Approach to the Document Access Problem of Insider Threat," (May 2005). IEEE Intl. Conference on Intelligence and Security Informatics.

Andersen, Cappelli, et. al., Software Engineering Institute. (February 2004). "Preliminary System Dynamics Maps of the Insider Cyber-threat Problem." PA: Carnegie Mellon University.

Anderson, R., Bozek, T., et. al. (August, 2000). "Conference Proceedings Research on Mitigating the Insider Threat to Information Systems #2: Workshop Proceedings," DC: National Defense Research Institute.

Anderson, R., and Brackney, R., RAND Corporation National Security Research Division (March 2004). "Understanding the Insider Threat: Proceedings of a Workshop" CA: RAND Corporation.

Band, S., Cappelli, D., Fischer, L., Moore, A., Shaw, E., and Trzeciak, R., Carnegie Mellon University Software Engineering Institute (December 2006). *Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis*. PA: Carnegie Mellon University.

Cappelli, D., Keeney, M., Kowalski, E., Moore, A., Randazzo, M. (August 2004). *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*, PA: Carnegie Mellon University.

Cappelli, D., Moore, A., and Shimeall, T., "Common Sense Guide to Prevention and Detection of Insider Threats" (2005) DC: US-CERT.

Cappelli, D., Keeney, M., Kowalski, E., Moore, A., Shimeal, T., Rogers, S. (May 2005). *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*. PA: Carnegie Mellon University.

Chinchani, R., Iyer, A., Ngo, H., and Upadhyaya S. "A Target-Centric Formal Model for Insider Threat and More," NY: State University of New York at Buffalo.

Cunningham, W., Ohlhausen, P., Oliver, L., Seamon, T. of Homeland Security (January 2005). *Enhancing Private Security Officer Surety*, DC: U.S. Government Printing Office.

Ellison, R., Moore, A. (March 2003.) "Trustworthy Refinement Through Intrusion-Aware Design (TRIAD)" PA: Carnegie Mellon University Software Engineering Institute.

Government Accountability Office. "Continuing Attention to Privacy Concerns Is Needed as Programs Are Developed" (2007). DC: U.S. Government Printing Office.

Gordon, L., Loeb, M., Lucyshyn, W., and Richardson, R. Computer Security Institute (2006). *CSI/FBI Computer Crime and Security Survey 2006.*

Heuer, J., Kramer, L., Crawford, K., (May 2005). *Technological, Social, and Economic Trends That Are Increasing U.S. Vulnerability to Insider Espionage*. CA: PERSEREC.

Post, J., Shaw, E., and Ruby, K. Political Psychology Associates, (June 1998). "The Insider Threat to Information Systems: The Psychology of the Dangerous Insider" *Security Awareness Bulletin*.

Rasmussen, G. "Insider Risk Management Guide" http://www.gideonrasmussen.com/article-13.html

U.S. Department of Defense. (September 2007). *Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software. DC: U.S. Government Printing Office.*

U.S. Department of Homeland Security. (2006). *National Infrastructure Protection Plan.* DC: U.S. Government Printing Office.

U.S. Department of Homeland Security, Science and Technology Directorate, (2007) *Domestic Municipal End-to-End Water Architecture Study*. DC: U.S. Government Printing Office.

U.S. Department of Justice, Office of the Inspector General. (March 2008). *Audit of The U.S. Department Of Justice Terrorist Watchlist Nomination Processes.* DC: U.S. Government Printing Office.

U.S. Department of Justice. (June 2006). *The Attorney General's Report on Criminal History Background Checks.* DC: U.S. Government Printing Office.

U.S. National Counterintelligence Executive (April 2005). *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—2004*. DC: US Government Printing Office.

U.S. National Security Agency: *The Insider Threat to U.S. Government Information Systems*, (July 1999). DC: U.S. Government Printing Office.

Verton, D. "Insider Threat to Security May Be Harder to Detect, Experts Say" (April 12, 2002) *Computerworld.*

APPENDIX C: NATIONAL INFRASTRUCTURE ADVISORY COUNCIL MEMBERS

NIAC CHAIR

Chair – Mr. Erle A. Nye, Chairman Emeritus, TXU Corporation
Vice Chair – Mr. Alfred R. Berkeley, III, Chairman and CEO, Pipeline Financial Group LLC, *(Vice Chairman (ret.) NASDAQ)*
Mr. Edmund G. Archuleta, President and CEO, El Paso Water Utilities
Dr. Craig R. Barrett, Chairman of the Board, Intel Corporation
Mr. George H. Conrades, Executive Chairman, Akamai Technologies
Lt. Gen. Albert J. Edmonds (ret.), Chairman, Edmonds Enterprise Services, Inc
Chief Gilbert G. Gallegos (ret.), Chief of Police, City of Albuquerque, New Mexico
Ms. Margaret E. Grayson, President, Coalescent Technologies Inc.
Commissioner Raymond W. Kelly, Police Commissioner, New York Police Department
Ms. Martha H. Marsh, President and CEO, Stanford Hospital and Clinics
Mr. James B. Nicholson, President and CEO, PVS Chemicals, Inc.
Mr. Thomas E. Noonan, Former General Manager, IBM, Internet Security Systems
Hon. Tim Pawlenty, Governor, State of Minnesota
Mr. Gregory A. Peters, CEO, M1 Global Solutions
Mr. Bruce Rohde, Chairman and CEO Emeritus, ConAgra Foods
Dr. Linwood H. Rose, President, James Madison University
Mr. John W. Thompson, Chairman and CEO, Symantec Corporation

APPENDIX D: RESOURCES

Subject Matter Experts Consulted During the Course of the Study

Mr. Charles Bartoldus, DHS Screening Coordination Office
Mr. Bob Belair, SEARCH
Ms. Dawn Cappelli, Carnegie Mellon University, CERT Coordination Center
Mr. Frank Campbell, Senior Counsel, Justice Department
Professor Fred H. Cate, Indiana University
Mr. Tom Donahue, Central Intelligence Agency
Mr. Maurice Emsellem, National Employment Law Project (NELP)
Dr. Michael Gelles, Deloitte and Touche
Mr. Michael Glass, Office of the National Counter Intelligence Executive (ONCIX)
Mr. James Gray, FBI Criminal Justice Information Service (CJIS)
Mr. Michael Greenwood, Carnegie Mellon University, SEI CERT Coordination Center
Mr. Rudy Guerin, Pamir Corporation
Mr. Ronald Hawley, SEARCH
Ms. Andrea Heintzelman, Terrorism Screening Center (TSC)
Mr. Rick Kopel, Terrorism Screening Center (TSC)
Mr. John Kopsky, Office of the National Counter Intelligence Executive (ONCIX)
Ms. Toby Levin, DHS Privacy Office
Ms. Margie Love, American Bar Association
Mr. Thomas Mahlik, FBI Domain Program
Professor Deirdre Mulligan, University of California, Berkeley Law School
Mr. John Porco, Michael Baker Group
Mr. Henry Reather, DoD Counter Intelligence Field Activity (CIFA)
Mr. Joe Ricci, National Association of Security Companies (NASCO)
Professor Stephen Saltzburg, American Bar Association
Dr. Eric Shaw, Clinical Psychologist
Ms. Donna Uzzell, Florida Department of Law Enforcement, Compact Council Chair
Ms. Kelli Ann Walther, DHS Screening Coordination Office
Ms. Gloria Zaborowski, FBI Domain Program

APPENDIX E: FRAMEWORK FOR EDUCATION AND AWARENESS OF THE INSIDER THREAT

As further guidance for the Education and Awareness program recommended by the NIAC, the NIAC developed the framework below to allow the study's findings to guide the development of this program.

I. Establish a common, baseline understanding of the Insider Threat to Critical Infrastructures among the executive leadership of CIKR operators in the U.S.
    a. Define the insider threat to critical infrastructures for executives
        i. Communicate the dynamic and emerging nature of the insider threat
        ii. Illustrate the CI interdependencies and potential public welfare risks involved
        iii. Demonstrate the difference between IT surveys and potential risk to critical assets
    b. Communicate *enterprise risk* potential of Operational insider threats
        i. Share process for identifying tangible and intangible critical assets – physical assets and public confidence
        ii. Models to identify gaps in current IT risk mitigation — the new approach.
            1. Self discovery approach to risk identification.
            2. best practices for IT mitigation (report annex)
        iii. Need for internal facing security measures –
            1. Discuss focus on external threats despite internal risks.
            2. Discuss culture of trust for long-term employees, seniority - cite evidence of insider cases with long term employees.
    c. Communicate *enterprise risk* potential of Economic Espionage insider threats
        i. Self discovery approach for identifying information assets – what information, if lost has the potential to bring down your company over time?
        ii. Discuss globalization and technology dynamics context for this threat, including risks involved in international operations, globalized networks, assessing personnel risks overseas, variation in privacy protection laws.
        iii. Discussion on IT (tech) risks and the culture of business that magnify these risks – they do it the way that they do and they don't want to change. Cultural discussion – there must be change to address this problem.
        iv. Share government information on growing international EE threat, companies and technologies targeted, resources for addressing this threat, more?
    d. Communicate mitigation approaches to insider threats
        i. Communicate types of threats and risk mitigation strategies (included in the report)
        ii. Best practices and resources for insider threat mitigation (screening, behavior observation, policy implementations to address insider situations)
        iii. Need for insider threat focused policy and components involved
        iv. Assigning security responsibilities to asset owners, not IT departments
        v. Communicate importance of cultural shift needed to address the emerging insider threat

vi. Importance of involving and educating key stakeholders, such as labor unions, during insider threat policy development process where necessary

e. Directions to resources available to CIKR operators for developing cost-appropriate risk mitigation programs
   i. Report's Best Practices Framework (below)
   ii. FBI Domain Program
f. Shared government (intelligence) agency information insider threats

II. Develop education and awareness programs for critical infrastructure workforce and management (elements include):
   a. Management awareness and training programs
      i. Training for Insider Threat Indicators
      ii. Illustration of Insider threat consequences – what is the insider threat to them?
         1. Highlight commonalities between workplace violence and insider threats – align insider threat issue with workplace safety
      iii. Establish clear understanding of consequences for reporting a colleague
         1. Create value in participation in EAP/ reporting, minimize costs for involvement
      iv. Make Employees Assistance Programs (EAP) a valuable option
      v. Elevate the value of your workers and their work to your company – provide a sense of purpose and belonging
         1. Importance of creating value and purpose with employees and the benefits derived from this approach (clearer view of threats, stronger workforce, etc.)
   b. Develop policy and authority to manage insider threat programs.
      i. Policy to support insider threat indicator mitigation
      ii. Align Employee Assistance Programs with security programs
      iii. Integrating Legal, HR (& EAP), Management, and Security in coordinating IT threat scenario approaches
   c. Mitigation approaches for insider threats
      i. Provide list of organizational resources developing insider threat policy and for dealing with insider threat scenarios
      ii. Provide recommended list of policies needed to mitigate insider threats and minimize litigation consequences
      iii. Reference best practice policy solutions for insider threats
      iv. Reference technology solutions and approaches to insider threat mitigation
      v. Outline importance of psychology in mitigation policy including issues such as:
         1. Importance of employee perceived self value in an organization – anti-social nature of insider threat behavior
         2. Physical security communicating security awareness to employees
         3. Clear communication and enforcement of boundaries
         4. The importance of involved, interactive security training for employees – can't be a check-box approach
         5. Establishing accountability for actions both physical and cyber

APPENDIX F: BEST PRACTICES FRAMEWORK FOR INSIDER THREAT MITIGATION

This annex presents the NIAC's compiled findings on insider threat mitigation strategies, which were identified over the course of the Study. Most critical infrastructure owners and operators do have policies in place for internal facing security, personnel safety, and hiring and termination, all of which address insider threats to some degree. Because critical infrastructures are so vital to our economic and public health security, CIKR operators should consider a more comprehensive approach to this threat and employ a risk management strategy.

The best practices framework that follows is structured similar to a risk management integrated framework for controls. Proper risk management controls are fashioned as a set of complementary protective provisions, which are layered in a "defense-in-depth" manner to protect vital assets. When an initial set of measures fails, such as initial employment screening, the succeeding layers of protection can prevent or mitigate catastrophic loss from an insider attack.

Controls include policies, procedures, practices, technologies and organizational structures, designed to provide reasonable assurance of achieving the business objective (insider threat mitigation here), as well as detection, prevention, and correction of undesired events. Good control design practices lead to effective execution and efficient testing and auditing. Effective controls should also: present clear, unambiguous description and formal procedure; align with risk and control objective; establish ownership for the control; as well as include audit trails, clear evidence of execution, and means of verifying performance of control for periodic certification and testing.

Integrated controls to mitigate insider threat risks should be the result of a cross-enterprise risk assessment. These assessments should focus on preventing, detecting, correcting potential actions of a malicious insider that could result in significant financial damage to the operator, such as: loss of operations; the ability to provide critical infrastructure services; shareholder or customer loss of confidence; and damage to brand image. Unlike other companies, CIKR operators should also give special consideration to threats that could cause wide scale damage outside their company, such as: "weaponization" of a critical infrastructure; geographic or cross-sector cascading CI service interruptions, prolonged CI service interruptions, damage to public health or welfare, loss of economic activity, or loss of public confidence in government or institutions.

<u>Sample Risk Controls Framework Measures</u>

1. Hiring Practices
    a. Develop clear risk assessments for different positions of trust within the company
        i. Develop understanding of risk for high-trust positions involving access and knowledge of high value, vulnerable systems, processes or facilities
        ii. Establish clear understanding of internal vulnerability and risk posed by access to company facilities and systems
    b. Develop a comprehensive risk-based screening policy to carefully evaluate all available information and establish an appropriate level of trust for an employment candidate
        i. Develop periodic re-investigation program for highly-trusted positions

ii. Policy should consider relevant, available screening information from sources including: reference checks, credit records, driving records, and criminal history records, (as regulated by applicable laws), as well as education and employment background information, etc.

c. Publish and adhere to clearly articulated background investigation process for employment candidates. Write policies to include:
   i. Screening policy, detailing hiring and adjudication process
   ii. Screening criteria used in adjudication for different positions
   iii. Applicant consent policy and notification process
   iv. Expectations for employee conduct
   v. Policy for periodic reinvestigation, where applicable

d. Develop employee screening and hiring practices with coordinated involvement of internal Legal, IT, Security, and Human Resources teams

e. Document and consistently apply hiring practice policies to minimize exposure to employment litigation

2. Human Resources Management Policies and Practices
   a. Develop HRM policies in coordination with internal legal, security and human resources team managers, and where applicable, with the resource manager for job specific policies
   b. Build a cross-departmental insider threat approach and response team, to include: IT, Physical Security, Legal, and Human Resources
   c. Use a real-time Human Resources Management System to maintain employee status and role information
      i. Integrate HRM System with IT, Physical Security Access, and Human Resource Management Systems to ensure terminated employees are consistently denied access, organization-wide
   d. Establish a strong Employee Assistance Program to help employees identify themselves and peers for assistance during high-risk periods of difficulty
      i. Minimize downside to employees for participation, such as demotion, or loss of employment or privacy
      ii. Include coordinated policy to appropriately scale employee access during high-risk periods, minimizing risk of sabotage
   e. Communicate expectations and standards for disciplinary action or dismissal
      i. Use (available/CERT) research findings to develop a process and a set of policies focused to protect assets and operations while dealing with a hostile insider
   f. Develop or review all internal facing security HR policies for potential negative effect on employee morale
3. Awareness Communications and Training
   a. Apply (available/CERT) research to develop programs and strategies for identifying at-risk behavior in high-trust positions as well as company-wide
   b. Seek to establish a work environment that communicates value and purpose to employees; maintain employee morale to make insider threats more visible
   c. Establish supervisor training programs for all supervisors, to include:
      i. Processes and standards for identifying potential problem employees

        ii. Procedures for handling potential insider threat problems and notification of human resources team
        iii. Expectations regarding
    d. Employees should be trained regarding expectations for ethics, professional conduct, computer use and access, and physical facilities access
4. Legal Policies and Practices
    a. Coordinate employee hiring, screening, and termination policies with legal team and asset owners/ risk managers to ensure legal team understands the potential costs of insider threats
    b. Establish a set of legal approaches and policies to address insider scenarios, in coordination with HR, Security, and IT
    c. Develop documents to establish accountability, e.g., employee's annual ethics certification, confidentiality agreements, supplier security requirements for contracts
    d. Coordinate legal perspective with asset owners and risk managers to develop clear understanding of insider threat consequences and costs
5. Coordinated Insider Threat Controls Program
    a. Appoint an insider threat manager responsible for
        i. Developing and implementing insider threat controls
        ii. Deploying insider threat technology solutions
        iii. Coordinating and implementing insider threat education and awareness programs
        iv. Reporting status of goals and objectives to CEO and corporate board
    b. Establish an insider threat response team, to include Legal, Human Resources, IT, and Security representatives, and add the relevant asset owner in each specific case
6. Identity Management Controls
    a. Use fingerprint criminal history checks to conclusively establish positive identification of employment candidates when possible
    b. Use redundant sign-on technologies to increase the security of sensitive Physical and IT systems (e.g. password/passcode and biometrics, access cards, encryption keys, etc.)
    c. Use security best practices measures to reduce the potential for stolen identification and access
7. Physical Security
    a. Coordinate security management with Insider Threat controls
    b. Apply internal security protections to mitigate high-consequence insider threat risks
    c. Integrate physical access control systems to coordinate with HR systems role and current status for each employee
    d. Use physical access information to identify access violations and abnormal behavior associated with insider threats
    e. Use an integrated Physical and IT security systems view to identify rule violation patterns for potential insider threat behavior
    f. Use a structured internal physical access control architecture to minimize access risks
        i. Trust-based layers to limit employee access to perimeter, outer and inner layers
        ii. Role-based access to high-risk functional areas

g. Use role-based over computer systems, operational facilities, other critical resources of an enterprise

8. IT Systems/Cyber Security
    a. Use integrated IT and Physical security systems tools to identify rule violation patterns for potential insider threat behavior
    b. Use dual protection access technologies (e.g. biometric, key card or encryption key verification to strengthen identity management on IT systems)
    c. Use dual controls access to protect high-value systems and processes from risk posed by a single rogue employee
    d. Integrate IT access controls with Human Resource Management System to manage access to, integrity and availability of computer systems (e.g., identity management system)
    e. Use segregation of duties for control over creation and termination of user and administrator accounts and maintaining security/access rights
        i. Use role-based access to computer system functions
        ii. Incorporate concepts such as least-privileged access, segregation of duties
    f. Set strength of login security dependent on extent of user/administrator privilege, e.g., eight-character passwords for low-level user access but two-factor authentication with smart card for administrator to login remotely
    g. Maintain best practices standards for software patching/security updates
    h. Maintain best practices standards for anti-virus, firewall, intrusion detection and internal intrusion detection as well as deterrence technologies
    i. Use best practice standards for critical IT systems and data backup and recovery
9. Contracting/Outsourcing Security Due Diligence
    a. Evaluate insider exposure and risks posed by contracted suppliers, vendors, and partners
        i. Use standards for establishing contractor trust and access
        ii. Include appropriate contract security requirements
        iii. Establish mechanism for monitoring contractor security oversight

APPENDIX G: SAMPLE BEST PRACTICES SCREENING POLICY - EMPLOYEE BACKGROUND INVESTIGATIONS AND ADJUDICATION

Screening Guidelines for New Hires

June 2007

Dominion conducts comprehensive background investigations on individuals seeking employment with the Company.

These background investigations are used to help make a determination of a candidate's eligibility for employment with Dominion. The background investigations are conducted by Dominion Security. The information is developed through the use of proprietary, public, and outside agency sources. All aspects of the company's program comply with the requirements of the Fair Credit Reporting Act.

Information collected during the process is maintained confidentially in a secure location. The information developed during the investigation will be provided only to appropriate company management and, upon request, may be reviewed by the candidate.

Background Investigations on applicants will include:

➢ Comprehensive Criminal History Check (all positions)

Security will check criminal history, and may disqualify for:

- Any felony convictions
- Any misdemeanor conviction for crime involving violent or aggressive behavior
- Any misdemeanor conviction for theft within the past ten years
- Any other misdemeanor conviction within the past seven years
- Any combination of two or more misdemeanor convictions within the past 10 years
- Any evidence based upon a pattern of convictions that suggests a disregard for laws and rules
- Any pending disposition regarding criminal activity

- **Currently serving a probationary period as a result of a criminal conviction**

➢ Credit Report Review (credit-sensitive positions only)*

Security will evaluate indicators of financial responsibility during past five years, and may disqualify for:

- Frequent and/or high dollar outstanding suits and judgements in **excess of $5,000**
- Unpaid tax liens
- A high percentage of stated accounts not in good standing, to include: collection accounts, accounts charged off to profit and loss, significant past due accounts, bad debt accounts, and current and previous negative accounts
- **A pattern of financial irresponsibility as demonstrated by bad debt accounts for non-essential items and services**
- Any unpaid collectable/bad debt with any Dominion company

(NOTE: All credit reporting will be evaluated carefully based upon the position, and considered with other information developed during the background investigation.)

➢ Driving History Review (all non-driver sensitive positions)

Security will check the five-year driving history, and may disqualify for:

- Two or more convictions within the last seven years of any combination of DUI/DWI, Hit and Run, or driving while license revoked or suspended; or a 2nd offense of any within the last five years, or **other egregious offenses**.
- "Habitual Offender" status noted on DMV report.
- Any pattern of disregard for rules and regulations, including multiple violations of motor vehicle laws, such as five or more speeding convictions within the past 24 months.

➢ Driving History Review (driver-sensitive positions only)**

Security will check the five-year driving history, and may disqualify for:

- Excessive point accumulation.
- No operator's license or an operator's license currently under suspension or revocation.
- Two or more convictions within the last seven years of any combination of DUI/DWI, Hit and Run, or driving while license revoked or suspended; or a 2nd offense of any within the last seven years, **or other egregious offenses.**

- Three or more speeding convictions within the past 24 months.
- "Habitual Offender" status noted on DMV report.
- Any pattern of disregard for rules and regulations, including multiple moving violations of motor vehicle laws.

➢ Employment and Education Verifications (all positions)***

Security will validate post high school degrees and certifications, and a minimum three-year work history (to include periods of unemployment), and may disqualify for:

- Negative employment references regarding job performance
- Employment terminations or forced resignations
- Falsification of information regarding dates and places of employment
- Falsification of education credentials

➢ Additional Areas of Consideration (all positions)

Security may disqualify for:

- Any falsification, omission, or misrepresentations on the employment application or release forms
- Any incident involving workplace violence, or other unacceptable workplace conduct
- Any information determined by Dominion to reflect a lack of trustworthiness

***Credit Sensitive positions** include those having financial or cash handling responsibilities, or having access to customer records or other sensitive information. These positions typically are found within the Credit Union, Accounting areas including Payroll Accounting, Accounts Receivable and Remittance Processing, Call Centers, Legal, Human Resources, Security, IT, and Nuclear. All management positions (supervisors and above) require a credit report review. Certain positions within the Clearinghouse (to include all energy traders) and in Supply Chain Management are also subject to a credit report review. Human Resources may also direct Security to run a full credit report by indicating such when initiating a background request. Security reserves the right to conduct full credit reviews on other positions as deemed necessary.

Driver Sensitive positions include those that require the employee to drive a Dominion-assigned vehicle or a personal vehicle on behalf of Dominion. These positions include meter readers, service representatives, security officers, and field employees.

***Security will validate** high school diplomas/GED's for positions in security and at the nuclear power stations.

****

Before forwarding paperwork to Security to initiate the background investigation, please ensure that:

- All fields are completed in a neat and legible manner
- All forms are signed and dated
- The specific date and location (county/state) of criminal activity are noted if a felony conviction is stated on the paperwork
- Complete driving record information is included regardless of position
- Any explanations provided by the applicant to clarify employment application responses are included
- Full employer name/location/contact information (on employment application) is stated for each current and previous employer

Contact supervisor, Security Services at (phone number) with questions.