Lishchynsky, M. (2025). The insider threat: A socio-technical analysis of preventing data breaches and espionage within governmental agencies. Politics & Security, 12(2), 88–103. Doi: 10.54658/ps.28153324.2025.12.2.pp.88-103

THE INSIDER THREAT: A SOCIO-TECHNICAL ANALYSIS OF PREVENTING DATA BREACHES AND ESPIONAGE WITHIN GOVERNMENTAL AGENCIES

Mykhailo Lishchynsky
State University of Information and Communication Technologies
Kyiv, Ukraine
https://orcid.org/0009-0009-0103-9904

Abstract *This article presents a socio-technical analysis of the insider threat phenomenon within governmental and public sector institutions. It argues that effective mitigation requires a dynamic, integrated strategy that moves beyond siloed technical controls to holistically address the interplay between individual psychology, organizational culture, technical architecture, and policy enforcement. The analysis defines the governmental insider threat, distinguishing between malicious, unintentional, and compromised insiders, and demonstrates how this typology maps to distinct root causes within the socio-technical system. Through a detailed examination of the Edward Snowden and Chelsea Manning cases, the article deconstructs the convergence of psychological, cultural, and technical vulnerabilities that precipitate catastrophic breaches. It systematically analyzes contributory factors at the individual level, using the Critical Pathway to Insider Risk (CPIR) model; the organizational level, focusing on culture, leadership, and trust; and the technical level, highlighting architectural weaknesses. The article then evaluates a multi-layered defense-in-depth framework integrating human-centric strategies (e.g., positive deterrence, robust training), technical countermeasures (e.g., Zero Trust Architecture, User and Entity Behavior Analytics), and comprehensive policy frameworks (e.g., Executive Order 13587, NITTF Maturity Framework). The inherent tension between security surveillance and employee privacy is explored, reframing privacy protection as a positive driver of organizational trust and security. The article culminates in a novel, coordinated intervention model and provides actionable policy recommendations for governmental agencies to build a more resilient and secure posture against the threat from within..*

Keywords: Insider Threat, Socio-Technical Systems, Government Security, Data Breaches, Espionage.

1. INTRODUCTION

Governmental agencies are built upon a fundamental paradox: the very trust required for their operation creates their most profound vulnerability. To function, these institutions must grant employees, contractors, and partners authorized access to sensitive facilities, systems, and, most critically, classified national security information (Greitzer et al., 2021). This act of entrustment, however, inherently creates the potential for an insider threat—a trusted individual who uses their legitimate access to cause harm, whether intentionally or unintentionally (Greitzer et al., 2021). This threat is not a modern anomaly but an enduring feature of human history, with a common narrative stretching from Benedict Arnold to the catastrophic unauthorized disclosures of the digital age (Greitzer et al., 2021). The core of the problem is fundamentally human; while technology enables new vectors for harm, the threat actor is a person, making the insider threat a "human problem" that demands a human-centric solution (Greitzer et al., 2021). Consequently, it must be understood as a complex socio-technical phenomenon, where risk emerges from the dynamic interplay of individuals, organizational structures, and technological systems (Hutchins et al., 2016).

To deconstruct this complexity, this article adopts a Socio-Technical Systems (STS) framework as its primary analytical lens. STS theory posits that organizational performance and security are not determined by technical or social elements in isolation, but by their joint optimization (Pasmore et al.,

2018). A purely technocentric approach to security, focused on firewalls and perimeter defenses, is demonstrably insufficient for countering the insider threat (Moore et al., 2015). Insiders, by definition, already possess the "keys to the kingdom" and can bypass external defenses (Silowash et al., 2012). Research consistently shows that human factors—such as behavioral choices, cultural norms, and cognitive errors—are paramount in the majority of security failures, whether in prevention, detection, or mitigation (Greitzer & Frincke, 2010). An STS approach, therefore, necessitates a holistic analysis that integrates insights from organizational psychology (to understand individual motivations and behaviors), public administration (to examine culture, leadership, and policy), and cybersecurity (to assess technical controls and architecture) (Nurse et al., 2014). An effective insider threat program cannot be merely "a security program"; it must be a "sustained employee outreach and awareness effort" that fosters a shared responsibility for protection (Greitzer et al., 2021).

The urgency of adopting a socio-technical perspective is amplified by an evolving threat landscape. The post-pandemic shift toward remote and hybrid work models has expanded the attack surface, fostering reliance on less-secure technologies and increasing employee isolation and stress—factors that can heighten vulnerability to exploitation (Greitzer et al., 2021). Simultaneously, foreign adversaries are engaged in an unprecedented effort to collect data on and exploit vulnerable individuals within critical infrastructure and government workforces, turning them into witting or unwitting assets (Greitzer et al., 2021). The increasing frequency and staggering financial impact of insider incidents, which can cost millions per event, underscore the inadequacy of legacy, perimeter-based security models and the critical need for more advanced, integrated defenses (Ponemon Institute, 2022).

A security strategy focused exclusively on malicious actors, who represent only one facet of the problem, will inevitably neglect the systemic factors that cultivate the far more common unintentional and negligent threats. Official definitions from the Cybersecurity and Infrastructure Security Agency (CISA) and the Office of the Director of National Intelligence (ODNI) explicitly include "unintentional" and "unwitting" harm, recognizing that negligence and accidents are significant contributors to overall risk (Greitzer et al., 2021). Research confirms that a majority of insider incidents stem from non-malicious actions and that many malicious insiders begin as loyal employees who are pushed down a path to betrayal by a combination of personal stressors and organizational failures (Cappelli, Moore, & Trzeciak, 2012). A security program that narrowly frames the problem as one of "finding and punishing bad guys" (Shaw, 2006) will fail to address the cultural, training, and system design flaws that enable the full spectrum of insider risk (Carroll, 2021).

Effective insider threat mitigation in the public sector requires a dynamic, integrated strategy that moves beyond siloed controls to holistically address the interplay between individual psychology, organizational culture, technical architecture, and policy enforcement. This article will deconstruct these socio-technical layers, analyze their interactions through historical cases and contemporary models, and synthesize a coordinated intervention framework to enhance agency resilience against the threat from within. The analysis begins by formally conceptualizing the governmental insider threat and establishing a typology based on intent. It then dissects high-profile breaches to reveal the anatomy of socio-technical failures. Following this, the report provides a multi-level analysis of contributory factors—individual, organizational, and technical. It then details an integrated prevention framework, combining human-centric, technical, and policy-based countermeasures. The enduring dilemma of balancing surveillance and privacy is then examined before the article concludes with a proposed best-practice model and actionable policy recommendations for governmental agencies.

2. CONCEPTUALIZING THE GOVERNMENTAL INSIDER THREAT

*Defining the Insider: From Trusted Colleague to Threat Vector***.** In the context of governmental agencies, an "insider" is formally defined as any person who has or has had authorized access to an organization's resources, including its personnel, facilities, information, equipment, networks, and systems (Greitzer et al., 2021). This definition is intentionally broad, encompassing not only direct government employees but also contractors, vendors, temporary staff, and other trusted business partners who are given access to perform their duties (US-CERT, 2012). The defining characteristic of the insider is their position of trust and the legitimate access it confers. The "insider threat" is the potential for that individual to use their

authorized access—wittingly or unwittingly—to cause harm (Greitzer et al., 2021). In the public sector, this threat is particularly acute because the harm can extend beyond organizational damage to compromise national security, public safety, and the integrity of government functions (Greitzer et al., 2021). The threat can manifest in numerous ways, including espionage, terrorism, sabotage, workplace violence, corruption, and the unauthorized disclosure of classified or sensitive information (Greitzer et al., 2021).

A Typology of Insiders: Differentiating Intent. A nuanced understanding of insider threats requires differentiating them based on the individual's intent, as the root causes and appropriate mitigation strategies vary significantly for each type. A comprehensive typology is therefore not merely descriptive but serves as a diagnostic tool for an organization's security posture. A high prevalence of accidental incidents, for example, points toward failures in training and system usability, whereas a pattern of malicious acts suggests deeper problems with organizational culture and employee well-being.

The malicious insider is an individual who intentionally uses their authorized access to harm the organization or misappropriate its assets (Carroll, 2021). Their motivations are diverse and can include financial gain (e.g., selling intellectual property), revenge for a perceived wrong (such as being passed over for a promotion), ideological alignment with an external cause, or espionage on behalf of a foreign entity (Carroll, 2021). Malicious insiders can be further categorized:

- *The Lone Wolf*: This individual acts alone, driven by personal grievances or ideology. They leverage their own knowledge of the organization's systems and security weaknesses to execute their attack and avoid detection (Carroll, 2021).
- *The Collaborator*: This insider works in collusion with an external party, such as a competitor or a criminal organization. They may be motivated by payment or coercion, providing the external actor with credentials, insider knowledge, or direct access to bypass security defenses (Carroll, 2021).

The Unintentional Insider. The *unintentional insider*, often representing the largest portion of insider-related incidents, is an individual who causes harm without malicious intent (Carroll, 2021). Their actions stem from carelessness, mistakes, or a lack of security awareness. This category is critical because it highlights vulnerabilities in processes, training, and culture rather than individual malevolence.

- *The Negligent Insider*: This person is generally aware of security policies but chooses to ignore or circumvent them for reasons of convenience or perceived efficiency. Examples include sharing passwords with colleagues, using unauthorized personal devices for work, or failing to install critical security patches (Greitzer et al., 2021). This behavior often points to a weak security culture or policies that are perceived as overly burdensome.
- *The Accidental Insider*: This individual causes a security incident through a genuine mistake. Common examples include sending a sensitive email to the wrong recipient, inadvertently clicking on a phishing link that installs malware, or misconfiguring a cloud storage setting, thereby exposing data (Greitzer et al., 2021). These incidents often reveal gaps in security awareness training and a need for more user-friendly, mistake-proof systems.

The Compromised Insider. The *compromised insider* is a legitimate user whose credentials or system access have been stolen by an external attacker (Carroll, 2021). The employee is an unwitting pawn, and their account is used to masquerade as a trusted entity within the network. This threat type blurs the line between external and internal attacks and underscores the critical importance of robust identity and access management controls. The attacker, operating with the insider's privileges, can access data, install malware, or move laterally through the network, often evading detection for extended periods (Sarkar et al., 2020).

Beyond a Binary: "Insiderness" as a Spectrum of Access and Trust. A sophisticated analysis must move beyond a simple binary distinction between "insider" and "outsider." Instead, *insiderness* should be conceptualized as a non-binary spectrum, where an individual's degree of insiderness is a function of their specific access privileges relative to a particular asset or resource (Bishop, 2005). For example, a senior systems administrator with root-level access to network servers is "more of an insider" with respect to that infrastructure than a policy analyst. However, that same policy analyst, who has access to draft national security directives, is "more of an insider" with respect to that sensitive information. This concept extends to physical access as well; a janitor with keys to a secure facility is an insider with respect to that

physical space (Bishop, 2005). This granular understanding is foundational to implementing the Principle of Least Privilege (PoLP), where access controls are tailored not just to a person's role, but to the specific data and resources they absolutely require to perform their duties. It shifts the security focus from a broad "trusted vs. untrusted" model to a more precise, asset-centric model of verifying access rights for every interaction.

3. ANATOMY OF A BREACH: SOCIO-TECHNICAL FAILURES IN HIGH-PROFILE CASES

An examination of seminal insider threat cases reveals the catastrophic potential of socio-technical failures. The breaches perpetrated by Edward Snowden and Chelsea Manning were not the result of a single vulnerability but rather a convergence of individual psychological pressures, permissive organizational cultures, and inadequate technical controls. They serve as foundational case studies demonstrating why a holistic, integrated approach to insider threat mitigation is imperative.

Case Study 1: Edward Snowden – The Social Engineer in a System of Assumed Trust

The 2013 disclosure of approximately 1.7 million classified documents by Edward Snowden, a former National Security Agency (NSA) contractor, exposed global surveillance programs and triggered a worldwide debate on security and privacy (Gelles, 2013). An analysis of the breach through a socio-technical lens reveals a systemic failure built on a flawed model of trust.

- *Socio-Psychological Factors*: Snowden's motivation appears to have been primarily ideological, driven by a belief that the surveillance programs he was exposed to were unconstitutional and that the public had a right to know (Gelles, 2013). This places him in the complex category of a prosocially motivated insider, acting to benefit what he perceived as a greater good ("society") rather than for personal gain or revenge (Gelles, 2013). His case highlights the critical role of whistleblower protections. At the time, legal protections for intelligence community contractors like Snowden were tenuous and lacked clear, enforceable legal rights, potentially leaving disclosure to the media as the only perceived viable channel for raising concerns (Fitzpatrick, 2021). This lack of a trusted internal reporting mechanism is a significant socio-policy failure that can push ideologically motivated insiders toward external disclosure.
- *Organizational & Cultural Vulnerabilities*: The most glaring vulnerability was the NSA's organizational culture. Snowden masterfully exploited a culture of collegial helpfulness to circumvent access controls. He used social engineering tactics, telling an estimated 20 to 25 coworkers that he needed their login credentials to perform his duties as a systems administrator, and they complied (Melley, 2014). This indicates a profound failure in security awareness and a culture where the social norm of helping a coworker overrode the cardinal security rule against sharing passwords. The incident suggests that security awareness training was "sorely lacking," as employees in one of the world's most secure environments fell for a basic social engineering trick (Melley, 2014).
- *Technical & Policy Vulnerabilities*: The Snowden breach was a direct result of "totally inadequate" policies and procedures (Melley, 2014). The primary technical failure was a breakdown in identity and access management. The system allowed for, and the culture tolerated, the sharing of login credentials. As a privileged user (systems administrator), Snowden already had significant access, but he was able to aggregate further privileges by using his colleagues' Public Key Infrastructure (PKI) certificates to access classified information on the NSANET (Gelles, 2013). This represents a complete violation of the Principle of Least Privilege. Furthermore, the systems in place lacked sufficient auditing and data exfiltration monitoring to detect and flag the anomalous activity of one user accessing data with multiple credentials and downloading vast quantities of information.

Case Study 2: Chelsea Manning – A Cry for Help in the Digital Panopticon

In 2010, Chelsea Manning, then a U.S. Army intelligence analyst stationed in Iraq, disclosed nearly 750,000 classified and sensitive military and diplomatic documents to the whistleblowing platform WikiLeaks (Greenwald, 2014). Her case illustrates how severe personal distress, when combined with an

unsupportive organizational environment and permissive technical access, can lead to a devastating security breach.

● *Socio-Psychological Factors*: Manning's actions were precipitated by a confluence of intense personal and professional stressors. She was grappling with her gender identity in a military environment governed by the "Don't Ask, Don't Tell" policy, which was hostile to LGBTQ+ service members and particularly to transgender individuals (Greenwald, 2014). This personal struggle was compounded by a profound moral conflict over the content of the information she was tasked with analyzing, which included videos of civilian casualties in Iraq and Afghanistan (Sontag, 2014). Her personal history, which included a difficult upbringing and being bullied, likely contributed to her feelings of alienation and a desire to act (Greenwald, 2014). Her disclosures can be interpreted as a dissident act of protection—"if you cannot protect me from my secrets, then I will not protect you from yours"—stemming from a feeling of being an "unprotectable" subject within the military's logic of security (Sontag, 2014).

● *Organizational & Cultural Vulnerabilities*: The organizational environment was a critical catalyst. Manning was described as "extremely isolated from her unit," indicating a significant failure of leadership, NCO supervision, and peer support systems (Sontag, 2014). Her defense team argued that supervisors failed to act on clear behavioral indicators of her mental and emotional distress, suggesting a breakdown in the military's duty of care and a failure to recognize that personnel well-being is a component of security (Sontag, 2014). The institutional culture, which at the time did not recognize or support transgender individuals, created an environment where her personal struggles were intensified rather than mitigated (Sontag, 2014).

● *Technical & Policy Vulnerabilities*: As a cleared intelligence analyst, Manning was granted broad access to classified databases, including the Secret Internet Protocol Router Network (SIPRNet) (Greenwald, 2014). The critical technical failure was the absence of effective data loss prevention (DLP) and endpoint monitoring controls. She was able to download hundreds of thousands of documents onto recordable CDs, which she reportedly labeled with titles like "Lady Gaga," without triggering any automated security alerts (Greenwald, 2014). This demonstrates a gaping vulnerability in monitoring data exfiltration to removable media. The system's security posture was predicated on trusting the cleared user, failing to scrutinize the user's behavior on the network. Access was granted based on role, not on a granular, need-to-know basis, and the system lacked the capability to detect and flag such a large and anomalous data transfer.

The Snowden and Manning cases, while different in motivation and method, both expose a fundamental flaw in legacy security models: the "trust-but-don't-verify" paradigm. Both individuals were granted enormous trust based on a static attribute—their security clearance. This initial grant of trust, a social and administrative construct, led to a dangerous relaxation of continuous technical verification. Snowden exploited the social layer of this trust, while Manning exploited the technical layer. The systems implicitly assumed that a trusted person would always behave in a trustworthy manner, a catastrophic miscalculation. These two breaches serve as the foundational justification for the shift toward a Zero Trust Architecture, which is built on the opposite principle: "Never Trust, Always Verify" (Rosenbach & Peritz, 2009).

Table 1: Comparative Analysis of Insider Threat Case Studies (Snowden & Manning)

Socio-Technical Dimension	**Case 1: Edward Snowden**	**Case 2: Chelsea Manning**
Insider Type & Motivation	Malicious (Ideological/Prosocial). Motivated by a belief that government surveillance was unconstitutional and a desire to inform the public (Greenwald, 2014).	Malicious (Moral/Psychological). Motivated by profound moral conflict over war conduct and severe personal distress related to gender identity and isolation (Sontag, 2014).
Psychological State	Principled dissent and a calculated decision to leak. Acted from a position of intellectual and ethical opposition to policy (Rosenbach & Peritz, 2009).	Extreme emotional distress, isolation, and moral injury. Actions were intertwined with a personal crisis and a cry for help (Sontag, 2014).

ISSN 2815-3324 Online, ISSN 2535-0358 Print

Socio-Technical Dimension	Case 1: Edward Snowden	Case 2: Chelsea Manning
Organizational Culture	Exploited a culture of collegial helpfulness that overrode security protocols. Security awareness was secondary to job expediency (Savage, 2016).	An unsupportive and isolating unit culture that exacerbated personal distress. A command climate that was hostile to gender non-conformity (Sontag, 2014).
Leadership & Peer Support	Colleagues were willing accomplices, albeit through social engineering. Indicates a lack of critical security thinking among peers (Savage, 2016).	Catastrophic failure of leadership and peer support. Supervisors allegedly ignored clear behavioral indicators of severe distress (Sontag, 2014).
Technical Vulnerability (Access Control)	Exploited weak identity controls by socially engineering colleagues for their credentials. Abused his privileged system administrator role to aggregate access (Greenwald, 2014).	Granted overly broad access to classified databases based on her role as an analyst. Lack of granular, need-to-know access restrictions on the network (Greenwald, 2014).
Technical Vulnerability (Data Exfiltration)	Inadequate auditing and monitoring to detect large-scale data harvesting from multiple user accounts. Focus was on perimeter, not internal activity (Greenwald, 2014).	Complete failure of endpoint security and Data Loss Prevention (DLP). Allowed mass download of data to removable media (CDs) without detection or prevention (Greenwald, 2014).
Policy Failure	Inadequate whistleblower protections for intelligence contractors, leaving external disclosure as a perceived viable option. Ineffective enforcement of policies against password sharing (Rosenbach & Peritz, 2009).	Lack of policies to support transgender service members. Failure to integrate personnel well-being policies with security protocols, treating them as separate issues (Sontag, 2014).
Primary Lesson	Static trust in credentials is a fatal flaw. Social engineering can defeat technical controls if the human element is untrained and the culture is permissive.	Personal well-being is a critical component of national security. Ignoring psychological distress in cleared personnel creates unacceptable risk.

4. A MULTI-LEVEL ANALYSIS OF CONTRIBUTORY FACTORS

To construct an effective defense, it is necessary to systematically deconstruct the factors that contribute to insider risk. A socio-technical analysis organizes these factors into three interconnected levels: the individual, the organizational, and the technical. These levels do not operate in isolation but form a dynamic feedback loop where vulnerabilities at one level can create or amplify risks at another.

4.1 THE INDIVIDUAL LEVEL: PSYCHOLOGICAL AND BEHAVIORAL DIMENSIONS

At the core of any insider incident is an individual. Understanding their psychological landscape and behavioral trajectory is crucial for detection and mitigation.

The Critical Pathway to Insider Risk (CPIR)

The Critical Pathway to Insider Risk (CPIR) is a widely accepted model in the insider threat community that provides a framework for understanding how a trusted individual transitions toward committing a harmful act (Shaw & Sellers, 2015)[1]. Developed by Dr. Eric Shaw, the model is not a rigid, linear progression but a flexible framework that describes an accumulation of risk over time (Shaw & Sellers, 2015; US CERT, 2012)[2]. The key components are:

- **Personal Predispositions:** These are the foundational vulnerabilities an individual brings to the organization. They include enduring personality traits (e.g., narcissism, low agreeableness, ethical flexibility), psychological conditions (e.g., substance abuse disorders), a history of rule violations, poor social skills, or significant personal vulnerabilities like financial instability (Shaw & Sellers, 2015). These factors do not destine an individual to become a threat, but they lower the threshold for them to react negatively to stressors.

- **Stressors:** These are the triggers—personal or professional—that can activate underlying predispositions and accelerate an individual's movement down the critical pathway. Professional stressors might include a poor performance review, being passed over for promotion, or interpersonal conflict with a supervisor. Personal stressors can include financial hardship, divorce, or the death of a family member (Shaw & Sellers, 2015).
- **Concerning Behaviors:** As an individual struggles to cope with the interaction of predispositions and stressors, they often exhibit observable behaviors that signal escalating risk. These can range from counterproductive work behaviors like absenteeism, tardiness, and poor performance to more alarming signs like expressions of disgruntlement, anger management issues, testing security boundaries, or unexplained affluence (Shaw & Sellers, 2015).
- **Problematic Organizational Response:** This is a critical, and often final, catalyst. How the organization responds to an employee's concerning behavior can either de-escalate the situation or push them further down the path. A heavy-handed, punitive, or dismissive response can intensify feelings of injustice and disgruntlement, while a supportive, fair, and proactive intervention can provide an "off-ramp" from the pathway (Vrieze, 2022)

Observable Behavioral Indicators

The CPIR model is operationalized through the observation of specific behavioral indicators. These fall into two broad categories: technical and psychosocial. Technical indicators are often captured by monitoring systems and include activities like accessing data at unusual hours, attempting to access unauthorized files, escalating privileges, using unapproved software, or downloading abnormally large volumes of data (Cappelli et al., 2012). Psychosocial indicators are observed through human interaction and can include increased disgruntlement and dissatisfaction, confrontational behavior, social withdrawal, expressions of divided loyalty, or signs of financial distress or substance abuse (Shaw & Sellers, 2015). A significant challenge is that many of these indicators are ambiguous on their own; an employee working late could be dedicated or preparing to exfiltrate data. Therefore, effective analysis requires gathering and integrating multiple indicators to see a converging pattern of risk (Greitzer et al., 2012).

Critiques and Limitations of Behavioral Models

While behavioral models like the CPIR are invaluable for framing the problem, they have limitations. The primary statistical challenge is predicting a low base-rate event; espionage and major sabotage are rare, making it difficult to build a predictive model with high accuracy and low false positives (Shaw & Sellers, 2015). The CPIR is a powerful heuristic for analysis and intervention, but it is not an infallible predictive tool. Critics and developers of the model acknowledge open questions regarding its full validation against agreed-upon criteria and the difficulty of precisely weighing the relative importance of different stressors and predispositions, which may interact in non-linear ways (Greitzer et al., 2012). The pathway is not always a simple, sequential progression, and organizational factors can be impactful at any point (Cappelli et al., 2012).

4.2 THE ORGANIZATIONAL LEVEL: CULTURE, LEADERSHIP, AND TRUST

The organization is not a passive backdrop but an active participant in the creation and mitigation of insider risk. Its culture, leadership, and approach to trust can either build resilience or cultivate the conditions for a breach.

Organizational Culture as a Security Control

Organizational culture—the shared beliefs, values, and norms that shape employee behavior—is a critical, albeit often overlooked, security control (Greitzer & Frincke, 2010). A toxic work environment characterized by perceptions of injustice, lack of support, or excessive pressure can directly cause or intensify the stressors that drive insider threats (Shaw & Sellers, 2015; Greitzer et al., 2012). Research shows a substantial relationship between employees' perception of injustice and deviant behavior like theft and sabotage (Willison & Warkentin, 2013). Conversely, a positive and "culturally competent" organization that values fairness, diversity, inclusion, and employee well-being fosters a sense of loyalty and psychological safety (Greitzer & Frincke, 2010). In such a culture, employees are more likely to internalize the organization's goals, voluntarily comply with security policies, and feel empowered to report concerns without fear of retaliation (Cappelli et al., 2012).

The Role of Ethical Leadership and Communication

Leadership is the primary architect of organizational culture (Greitzer & Frincke, 2010). In the context of public administration, ethical leadership grounded in principles of honesty, justice, respect, integrity, responsibility, and transparency is foundational to building public trust and ensuring effective governance (Brown & Treviño, 2006). This extends directly to insider threat mitigation. Leaders who model ethical behavior and communicate the importance of security and integrity set a powerful tone from the top (Shaw & Sellers, 2015). Communication must be clear, consistent, and transparent, especially regarding security policies and monitoring practices (Willison & Warkentin, 2013). Explaining the "why" behind security measures helps build buy-in and prevents the insider threat program from being perceived as a punitive, distrustful "Big Brother" initiative, thereby fostering the trust necessary for its success (Shaw & Sellers, 2015).

The Trust-Control Paradox

Government agencies face an inherent tension between the need to trust employees and the need to implement controls—the trust-control paradox. While trust is essential for morale and operational effectiveness, unchecked trust is a vulnerability. However, implementing overly intrusive surveillance and controls can erode morale, damage the psychological contract, and foster a culture of suspicion (Cappelli et al., 2012). This can be counterproductive, creating the very disgruntlement and resentment that the program aims to prevent. The key is to strike a defensible balance by achieving “proportionality” in surveillance, focusing monitoring on high-risk activities and critical assets rather than blanket observation, and being transparent about the process (Cappelli et al., 2012).

4.3 THE TECHNICAL LEVEL: SYSTEMIC AND ARCHITECTURAL VULNERABILITIES

Technical systems and their architecture can either provide robust defenses or create fertile ground for insider threats to flourish.

- *The Principle of Least Privilege (PoLP)*

A foundational source of technical vulnerability is the systemic failure to enforce the Principle of Least Privilege. Insiders, both malicious and unintentional, often have access privileges far exceeding what is necessary for their job functions (Cappelli et al., 2012). This “privilege creep” occurs through common but dangerous practices like permission inheritance, where a new employee’s access rights are simply cloned from a colleague’s profile, or the failure to revoke temporary, elevated privileges after a specific task is completed (Cappelli et al., 2012). Every unnecessary permission is an attack vector waiting to be exploited.

- *Insufficient Access Control and Auditing*

Weaknesses in Identity and Access Management (IAM) are a primary technical enabler of insider threats. A lack of strictly enforced multi-factor authentication (MFA) makes it significantly easier for an attacker to use compromised credentials, whether they were stolen from the insider or by the insider from a colleague (Cappelli et al., 2012). Compounding this is the problem of inadequate auditing. Without comprehensive and centralized logging of user activities—such as file access, system commands, and network connections—and the tools to analyze these logs for anomalies, it becomes nearly impossible to detect malicious or high-risk behavior in a timely manner (Brdiczka et al., 2012).

- *Data Exfiltration Pathways*

Finally, technical vulnerabilities manifest as open pathways for data exfiltration. These include unsecured endpoints that allow the connection of unauthorized removable media like USB drives, which was a key failure in the Manning case (Brdiczka et al., 2012). They also include poorly monitored network egress points, where large data transfers can go unnoticed. A significant and growing vulnerability is the use of *shadow IT*—unsanctioned cloud services, messaging apps, or other software that employees use to circumvent official, more restrictive channels, thereby bypassing security controls entirely (Greitzer & Frincke, 2010).

The interaction between these three levels is not linear but cyclical. A technical vulnerability, such as the ability to download data to a USB drive, provides an opportunity. An individual experiencing financial stress may have the motivation to exploit it. However, it is the organizational culture that acts as the critical modulator. A supportive culture may provide the employee with an off-ramp, such as an employee

assistance program, constraining the behavior. A toxic culture may amplify the motivation, encouraging the act. If the act is attempted and the organization's response is weak, it provides positive reinforcement, encouraging further, more severe actions and completing a dangerous feedback loop. This demonstrates that technical controls alone are insufficient; the "blast radius" of a technical flaw is ultimately determined by the organizational environment in which it exists.

5. AN INTEGRATED FRAMEWORK FOR PREVENTION AND MITIGATION

An effective defense against the insider threat cannot rely on a single solution but requires a multi-layered, defense-in-depth strategy that integrates human-centric, technical, and policy interventions. This socio-technical framework addresses risk at every stage, from preventing individuals from starting down the critical pathway to mitigating the impact of an incident that has already occurred.

5.1 HUMAN-CENTRIC STRATEGIES: THE FIRST LINE OF DEFENSE

Because the insider threat is a human problem, the most effective strategies begin with the workforce itself. The goal is to build a resilient, security-conscious culture that acts as the first and most crucial line of defense.

- *Effective Security Awareness and Training*

Annual, "check-the-box" security training is insufficient. An effective program requires a continuous vigilance campaign that keeps security top-of-mind. Best practices, as promoted by the Center for Development of Security Excellence (CDSE), involve using a variety of engaging methods, including real-world case studies, interactive games, and frequent, targeted messaging through multiple channels (CDSE, 2021). The primary objective of this training is to move beyond mere compliance and cultivate a proactive security culture. It aims to empower every employee to function as part of a "human sensor" network, capable of recognizing the behavioral and technical indicators of a potential threat and knowing how to report them through trusted, confidential channels (CISA, 2022).

The Formal Insider Threat Program (ITP)

As mandated by federal policy, a formal, centralized Insider Threat Program (ITP) is the organizational cornerstone of this strategy. An effective ITP is not just a security function but a multi-disciplinary hub that brings together expertise from Human Resources, legal counsel, privacy and civil liberties officers, security, counterintelligence, and information technology (Greitzer & Frincke, 2010). Governed by a designated senior official with clear authority and resources, the program's mandate is to gather, integrate, and analyze information from across the organization to detect potential threats (NITTF, 2020). Crucially, the program's philosophy should be geared toward proactive mitigation and intervention. The goal is to identify individuals who are on the critical pathway and provide "off-ramps"—such as counseling, financial assistance, or managerial intervention—to resolve the underlying issues before they escalate into a security incident. The mantra is to "turn people around, not turn them in" (Shaw & Sellers, 2015).

- *Positive Deterrence*

Complementing the formal controls of an ITP is the strategy of positive deterrence. This approach seeks to reduce insider risk not through fear of punishment (negative deterrence) but by aligning the interests of the employee with those of the organization. It is rooted in organizational psychology and focuses on increasing Perceived Organizational Support (POS)—the employee's belief that the organization values their contribution and cares about their well-being. Agencies can foster POS through practices such as ensuring procedural and distributive justice (fairness in processes and outcomes), providing robust employee support and development programs, and training managers to be supportive and respectful (Cohen, 2021). By reducing the disgruntlement, stress, and feelings of injustice that often motivate malicious acts, positive deterrence increases voluntary compliance with security policies and builds a more loyal, engaged, and resilient workforce (Shaw et al., 1998).

- *Whistleblower Protections*

A robust, accessible, and trusted whistleblower protection program is a critical safety valve within a governmental agency. When employees believe they have a legitimate and safe channel to report waste,

fraud, abuse, or other misconduct, it can prevent them from concluding that an unauthorized public disclosure is their only recourse (Shaw & Sellers, 2015). The Snowden case, in part, highlights the potential consequences of inadequate protections for contractors within the intelligence community (Pope, 2019). Strong protections are not antithetical to security; they are a component of an ethical and transparent culture that builds trust and can preempt damaging leaks by providing an alternative, sanctioned path for dissent.

5.2 TECHNICAL COUNTERMEASURES: BUILDING A RESILIENT ARCHITECTURE

Human-centric strategies must be reinforced by a robust technical architecture designed to limit opportunity and detect anomalous behavior. Modern defenses move beyond static, perimeter-based models to adopt dynamic, data-centric approaches.

- *Monitoring and Analytics (UEBA & DLP)*

• User and Entity Behavior Analytics (UEBA): UEBA solutions are a cornerstone of modern insider threat detection. These systems use machine learning and advanced analytics to establish a dynamic baseline of normal behavior for each user and entity (e.g., servers, devices) on the network. They then continuously monitor for deviations from this baseline. For an insider threat, this is critical for detecting actions that are technically authorized but behaviorally anomalous—for example, a network administrator who suddenly begins accessing large numbers of HR files at 3:00 AM (CISA, 2022). UEBA is particularly effective at identifying compromised credentials, as the external attacker's behavior will almost certainly differ from that of the legitimate user (King, 2022).

• Data Loss Prevention (DLP): DLP technologies are designed to prevent the unauthorized exfiltration of sensitive data. They function by first identifying and classifying sensitive data (e.g., classified information, Personally Identifiable Information (PII)) and then enforcing policies to control its movement. A DLP system can monitor data at rest (on servers), in use (on an endpoint), and in motion (across the network) (Pomerleau, 2021). It can automatically block an employee from emailing a classified document to a personal account, copying sensitive files to an unauthorized USB drive, or uploading them to a non-sanctioned cloud service (Watson, 2020). While implementation can be complex and face delays in large government environments, when operational, DLP provides a critical technical backstop against data breaches (DoD Cyber Exchange, 2022).

- *The Zero Trust Mandate*

The most significant strategic shift in government cybersecurity is the mandate to adopt a Zero Trust Architecture (ZTA), as directed by Executive Order 14028 (Office of the President, 2021). ZTA represents a fundamental paradigm shift away from the flawed "trust but verify" model.

• Core Principles: The foundational tenets of ZTA are "Never trust, always verify," the Principle of Least Privilege, and micro-segmentation (NIST, 2020). A ZTA assumes the network is already compromised ("assume breach") and therefore scrutinizes every single access request. Trust is never granted implicitly based on network location (i.e., being "inside" the firewall) or a one-time login (Walsh, 2021).

• Application to Insider Threats: ZTA is a powerful countermeasure to insider threats. By enforcing least privilege access, it ensures an insider can only access the specific data and applications they need to do their job, dramatically reducing the potential damage they can cause. Micro-segmentation prevents an insider (or a compromised account) from moving laterally across the network to access other systems. Most importantly, ZTA replaces the static trust model that failed in the Snowden and Manning cases with a system of continuous, dynamic authentication and authorization. Every request to access a resource is re-evaluated in real-time based on the identity of the user, the health of their device, the location, and other contextual signals (DoD CIO, 2022). The Department of Defense's comprehensive ZTA implementation strategy serves as a key roadmap for other agencies (Office of the President, 2021).

5.3 POLICY AND LEGAL SCAFFOLDING: MANDATES AND FRAMEWORKS

The human and technical strategies operate within a comprehensive policy and legal framework established to govern insider threat programs across the U.S. government.

- *Executive Order 13587 and the National Insider Threat Policy*

Issued in the wake of major leaks, Executive Order 13587 is the foundational directive for federal insider threat programs. It mandates that all executive branch agencies with access to classified information establish programs to deter, detect, and mitigate insider threats (Office of the President, 2011). The accompanying National Insider Threat Policy sets forth minimum standards, including requirements for monitoring user activity on classified networks, providing comprehensive employee awareness training, establishing a multi-disciplinary analysis hub, and ensuring robust protections for privacy, civil rights, and civil liberties (White House, 2012).

- *The NITTF Maturity Framework*

To help agencies move beyond simple compliance, the National Insider Threat Task Force (NITTF) developed the Insider Threat Program Maturity Framework. This framework provides a detailed roadmap for continuous improvement, outlining 19 maturity elements across key areas such as program leadership, personnel, training, access to information, user activity monitoring, and data analytics (NITTF, 2018). It allows agencies to self-assess their capabilities against best practices and identify specific areas for investment and enhancement, fostering a more proactive and effective security posture (NITTF, 2018).

- *Program Evaluation*

A critical policy component is the requirement for effective program evaluation. This presents a significant challenge, as "magic metrics" do not exist (CISA, 2022). Effective evaluation requires moving beyond simple operational metrics (e.g., number of alerts generated, cases closed) to develop programmatic metrics that measure actual risk reduction and alignment with organizational objectives (CISA, 2022). While it is difficult to prove how many incidents were prevented, a mature program can demonstrate its value through indicators of reduced vulnerability, faster detection times, and successful, non-punitive interventions. Meaningful metrics are essential for justifying program resources and maintaining support from senior leadership (CISA, 2022).

The strategies of positive deterrence and Zero Trust, while seemingly operating at opposite ends of the trust spectrum, are not contradictory but deeply synergistic. Positive deterrence aims to build social and psychological trustworthiness in the human actor, reducing their intent to cause harm. Zero Trust eliminates implicit technical trust in the system, continuously verifying the actor's access regardless of their intent. An employee cultivated in a high-trust, supportive environment is less likely to try to circumvent ZTA controls and more likely to understand their necessity. In turn, ZTA provides the hard guardrails that contain the damage from the rare malicious actor or the more common accidental error. A truly mature program integrates both, using culture to reduce the likelihood of an attempt and architecture to reduce the impact of any attempt that occurs.

6. THE ENDURING DILEMMA: BALANCING SURVEILLANCE, PRIVACY, AND TRUST

The implementation of any effective insider threat program inevitably confronts one of the most challenging ethical and legal dilemmas in modern governance: the balance between the state's need for security surveillance and the public employee's right to privacy. Navigating this conflict is not merely a matter of legal compliance but is central to the program's ultimate success or failure.

- *The Legal and Ethical Landscape*

In the United States, public sector employees do not forfeit all privacy rights at the workplace door. The Fourth Amendment provides protection against unreasonable searches and seizures, a principle that the Supreme Court has extended to the workplace in cases like *O'Connor v. Ortega*, which established that employees may have a reasonable expectation of privacy, balanced against the government's legitimate interests in supervision, efficiency, and security (Department of Justice, 2021). This balance is further governed by a complex web of statutes, such as the Privacy Act of 1974, which regulates the government's collection and use of personally identifiable information (U.S. Congress, 1974). From an ethical standpoint, any monitoring must be necessary and proportionate to the risk being mitigated; it cannot be a boundless digital fishing expedition (Wright & Kreissl, 2014).

- *The Psychological Impact of Surveillance*

The implementation of surveillance technologies, if handled poorly, can have a profoundly negative psychological impact on the workforce. Pervasive or opaque monitoring can create a "chilling effect," where employees alter their behavior and censor their communications out of fear of being watched or misinterpreted (Kamal, 2016). This erodes morale and fosters a culture of mistrust, directly undermining the psychological contract between the employee and the organization (Carroll, 2019). This outcome is not only detrimental to productivity and well-being but is actively counterproductive to the goals of the insider threat program. A workforce that feels constantly suspected and distrusted is more likely to become disgruntled, creating the very psychological conditions that can lead to insider threats (Cappelli, Moore, & Trzeciak, 2012).

- *Strategies for Achieving a Defensible Balance*

Striking a sustainable and legally defensible balance requires a deliberate, principled approach that integrates privacy protection into the very design of the insider threat program. This reframes privacy not as an obstacle to security, but as a critical enabler of it. When employees trust that their privacy is being respected, they are more likely to trust the organization and its security mission, leading to greater engagement, higher morale, and an increased willingness to act as partners in security by reporting genuine threats. This creates a virtuous cycle: robust privacy practices build employee trust, which in turn reduces malicious intent and increases voluntary reporting, thereby enhancing overall security.

Key strategies for achieving this balance include:

- Transparency and Communication: Agencies must be unequivocally transparent with their workforce about monitoring activities. This includes establishing clear, accessible policies that detail what information is collected, for what specific security purposes it is used, how it is protected, and who can access it (Cappelli, Moore, & Trzeciak, 2012). This transparency should be reinforced through mandatory training and conspicuous network login banners that inform users of monitoring for lawful government purposes (Executive Office of the President, 2011).
- Proportionality and Data Minimization: The scope of monitoring must be proportional to the risk. The goal is to protect the organization's "crown jewels," not to engage in "Big Brother" surveillance of the entire workforce (Cappelli, Moore, & Trzeciak, 2012). This principle of data minimization dictates that agencies should only collect and retain the specific data necessary to identify high-risk indicators, and for no longer than required (Department of Justice, 2021). Risk-based monitoring, which focuses on high-privilege users or anomalous activities, is preferable to indiscriminate surveillance.
- Oversight and Due Process: A multi-disciplinary governance body, which must include officials from the Office of General Counsel and the agency's privacy and civil liberties offices, is essential for providing independent oversight (Office of the Director of National Intelligence, 2017). This body must review and approve monitoring policies to ensure they are legally and ethically sound. Furthermore, there must be a clear, fair, and documented process for investigating alerts generated by monitoring systems, with avenues for employees to contest findings and correct inaccuracies in their records (Wright & Kreissl, 2014).
- Privacy Impact Assessments (PIAs): Before deploying any new monitoring technology, agencies should be required to conduct a thorough Privacy Impact Assessment (Department of Justice, 2021). A PIA is a formal process used to identify and mitigate potential privacy risks, ensuring that the technology's security benefits are weighed against its impact on individual privacy and that appropriate safeguards are built in from the start.

7. CONCLUSION: A COORDINATED MODEL FOR MINIMIZING INSIDER RISK

The insider threat is an enduring and complex challenge for governmental agencies, rooted in the paradox of trust. This analysis has demonstrated that the threat is not a monolithic problem solvable by a single tool or policy, but a multifaceted socio-technical phenomenon. The catastrophic breaches perpetrated by individuals like Edward Snowden and Chelsea Manning were not simple technical failures or isolated acts of troubled individuals; they were systemic breakdowns resulting from the convergence of psychological vulnerabilities, permissive organizational cultures, and inadequate technical and policy guardrails

(Brackney & Anderson, 2004; Shaw & Sellers, 2015). Effective prevention and mitigation, therefore, demand a departure from siloed, technocentric approaches. A resilient defense must be built on an integrated framework that jointly optimizes human, technical, and policy interventions, recognizing that these elements are inextricably linked in a dynamic system. A failure in one domain, such as a toxic culture, can neutralize the effectiveness of even the most advanced technical controls (Cappelli, Moore, & Trzeciak, 2012).

To translate this socio-technical imperative into an operational strategy, this article proposes a Coordinated Human–Technology–Policy Intervention Model. This model, detailed in Table 2, provides a holistic, defense-in-depth framework for insider risk management. It structures interventions across three critical domains—Human-Centric, Technical Controls, and Policy & Governance—and applies them at each stage of the risk lifecycle: Prevention & Deterrence, Detection & Analysis, and Mitigation & Response. This integrated model moves beyond a simple checklist of best practices to illustrate how different interventions must be coordinated to be effective. For example, preventing insider threats requires not only Zero Trust architecture (technical) but also a culture of psychological safety (human) and clear acceptable use rules (policy) (Department of Defense, 2023; Office of the Director of National Intelligence, 2017; National Insider Threat Task Force, 2020). By mapping interventions in this way, the model provides a practical and comprehensive roadmap for agency leaders and program managers to table2.

Table 2: A Coordinated Human–Technology–Policy Intervention Model for Insider Risk

Stage of Risk Management	A. Human-Centric Interventions	B. Technical Controls	C. Policy & Governance
1. Prevention & Deterrence	**Build a Resilient Workforce:** • Implement continuous, engaging, and behavior-based security awareness training and vigilance campaigns (CDSE, 2020). • Foster a culture of psychological safety, trust, and fairness through ethical leadership and supportive management (DeGraaf et al., 2018). • Actively promote Employee Assistance Programs (EAPs) and other wellness resources to provide "off-ramps" for stressed employees (Shaw & Sellers, 2015). • Implement "positive deterrence" strategies to align employee and organizational interests and reduce disgruntlement (Lind et al., 2001).	**Harden the Architecture:** • Implement a Zero Trust Architecture (ZTA) based on the principles of "never trust, always verify," least privilege, and micro-segmentation (Kindervag, 2010; Executive Office of the President, 2021). • Enforce strong Identity and Access Management (IAM), including mandatory phishing-resistant Multi-Factor Authentication (MFA) for all users (CISA, 2021). • Secure endpoints by controlling the use of removable media and unsanctioned software ("shadow IT") (Greitzer et al., 2012). • Classify all sensitive data and apply encryption at rest and in transit (Ponemon Institute, 2023).	**Establish Clear Guardrails:** • Develop and enforce clear, unambiguous policies for acceptable use, data handling, and remote work (Solove, 2008). • Mandate and resource a formal, multi-disciplinary Insider Threat Program (ITP) with a designated senior official (ODNI, 2017). • Establish and promote a trusted, accessible, and legally robust Whistleblower Protection Program (Devine, 2015). • Conduct thorough pre-employment screening and continuous vetting for all personnel with privileged access (NITTF, 2020).
2. Detection & Analysis	**Empower the Human Sensor Network:** • Train all personnel to recognize and report concerning behavioral and technical indicators via clear, confidential channels (CDSE, 2020). • Utilize the Critical Pathway to Insider Risk (CPIR) model as an analytical framework for the ITP hub to assess cases (Shaw & Sellers, 2015). • Involve behavioral science professionals in the analysis hub to help contextualize behaviors and reduce bias (NITTF, 2020). • Foster supervisor skills in recognizing and addressing concerning conduct early and appropriately (NITTF, 2020).	**Enable Data-Driven Visibility:** • Deploy and integrate User and Entity Behavior Analytics (UEBA) and Data Loss Prevention (DLP) tools (Gartner, 2023). • Use AI/ML to baseline normal user behavior, detect significant deviations, and assign risk scores to prioritize alerts (Ponemon Institute, 2023). • Correlate technical alerts from network, endpoint, and application logs with data from HR systems (e.g., performance reviews) and physical access logs (ODNI, 2017). • Maintain comprehensive, centralized, and attributable audit logs for all critical systems (CDSE, 2020).	**Define Analytical Governance:** • Mandate information sharing across agency silos (HR, Security, IT, Legal) to the central ITP analysis hub (ODNI, 2017). • Conduct Privacy Impact Assessments (PIAs) for all monitoring and analytics tools to ensure compliance and proportionality (Gellman, 2013). • Adhere to the NITTF Maturity Framework to guide the evolution of analytical capabilities (NITTF, 2020). • Establish formal procedures for validating and integrating new data sources into the analytical process (NITTF, 2020).

Stage of Risk Management	A. Human-Centric Interventions	B. Technical Controls	C. Policy & Governance
3. Mitigation & Response	**Prioritize Human-Centered Intervention:** • For non-malicious incidents, focus on corrective action, retraining, and addressing root causes (e.g., process flaws, usability issues) (Greitzer & Frincke, 2010). • For at-risk individuals, deploy supportive interventions (e.g., EAP referral, managerial support) to provide an "off-ramp" from the critical pathway (Shaw & Sellers, 2015). • Ensure all interactions are handled with fairness and respect to avoid exacerbating disgruntlement (avoid "problematic organizational responses") (Brackney & Anderson, 2004). • Maintain open communication with the workforce about the program's positive outcomes and supportive mission (DeGraaf et al., 2018).	**Execute Automated & Manual Response:** • Use Security Orchestration, Automation, and Response (SOAR) to automate initial responses to high-confidence alerts (CISA, 2021). • For active investigations, dynamically adjust access controls, increase monitoring levels, or isolate compromised systems to contain damage (ODNI, 2017). • Conduct thorough digital forensics to determine the full scope of an incident and preserve evidence (NITTF, 2020). • Ensure the ITP itself is audited to prevent misuse of powerful monitoring tools by its own personnel (NITTF, 2020).	**Ensure Legal & Procedural Integrity:** • Operate under a formal, legally vetted Incident Response Plan that defines roles, responsibilities, and escalation paths (NIST, 2018). • Ensure all mitigation and response actions are conducted with oversight from legal counsel and privacy officials to protect individual rights (ODNI, 2017). • Document all cases, actions, and outcomes in a secure case management system to ensure accountability and enable longitudinal analysis (NITTF, 2020). • Use after-action reports from incidents and exercises to drive continuous improvement of policies, procedures, and controls (NIST, 2018).

8. ACTIONABLE POLICY RECOMMENDATIONS FOR GOVERNMENTAL AGENCIES

Based on the preceding analysis and the integrated model, the following policy recommendations are proposed to strengthen insider threat mitigation across the public sector:

1. *Mandate a Socio-Technical Approach in Program Design and Evaluation.* Federal policy, including updates to the National Insider Threat Policy and agency-specific directives, should explicitly require Insider Threat Programs (ITPs) to be designed, implemented, and evaluated based on a socio-technical framework. This entails moving beyond a checklist of minimum technical standards toward demonstrating how human-centric strategies, technical controls, and policy governance are integrated into a cohesive, mutually reinforcing system. Oversight bodies should assess not only technical capabilities but also the maturity and coherence of this integration (Shaw & Sellers, 2015; NITTF, 2020).

2. *Elevate and Invest in Organizational Culture as a Security Metric.* Agencies should be required to treat organizational culture and psychological safety as core security concerns. This includes allocating resources for ethical leadership development, fostering procedural justice, and creating fair and psychologically safe work environments (Lind et al., 2001). Tools like the Federal Employee Viewpoint Survey (FEVS) should be formally integrated into insider threat assessments, and ITPs must collaborate with Human Resources to respond to organizational climate weaknesses (DeGraaf et al., 2018).

3. *Accelerate and Fully Fund the Zero Trust Mandate.* Congress and the Office of Management and Budget (OMB) must prioritize and enforce comprehensive implementation of Zero Trust Architecture (ZTA) across all agencies. ZTA must be recognized as foundational to insider threat prevention, not merely a cybersecurity upgrade. Its deployment should encompass all pillars of the CISA Zero Trust Maturity Model and be integrated into broader agency transformation initiatives (CISA, 2021; Executive Office of the President, 2021).

4. *Professionalize the Insider Threat Workforce.* The National Insider Threat Task Force (NITTF), in partnership with the Office of Personnel Management (OPM), should establish a formal certification and career development track for insider threat professionals. Given the cross-disciplinary nature of insider threat detection and response, training should include cybersecurity, behavioral science, data analytics, organizational psychology, counterintelligence, and privacy law (CDSE, 2020; NITTF, 2020). Standardized curricula should be developed and mandated for all ITP staff.

5. *Strengthen and Actively Promote Whistleblower Protection Channels***.** Inspector General offices should, in partnership with ITP leaders, conduct biennial audits of whistleblower protection programs to assess accessibility and effectiveness. Results should be reported to agency leadership and used to inform reforms. Awareness campaigns and training must frame protected reporting channels as legitimate, trustworthy, and central to the organization's mission—not as adversarial mechanisms (Devine, 2015; Greitzer et al., 2012).

6. *Adopt a "Balanced Deterrence" Policy.* The National Insider Threat Policy should mandate agencies to adopt and assess "positive deterrence" strategies in tandem with traditional security controls. Metrics of insider threat program success must include not only threats detected or incidents responded to but also improvements in employee morale, trust, and organizational support. A well-functioning ITP should be as much a proactive support structure as a reactive enforcement mechanism (Shaw & Sellers, 2015; Lind et al., 2001).

REFERENCES

Ablon, L. (2018). *Assessing the insider threat: Insights from past and present*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR4226.html

Allen, J., & Harper, A. (2020). *IT governance and risk management*. CRC Press.

Andress, J. (2019). *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice* (3rd ed.). Syngress.

Bada, A., Sasse, M. A., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint* arXiv:1901.02672.

Center for Development of Security Excellence (CDSE). (2020). *Insider threat training guide*. https://www.cdse.edu

Center for Internet Security (CIS). (2020). *Controls v8*. https://www.cisecurity.org

CISA. (2021). *Zero Trust Maturity Model*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/zero-trust-maturity-model

DeGraaf, G., Huberts, L., & Smulders, R. (2018). Understanding the research–practice gap in integrity and anti-corruption: The case of the Netherlands. *Public Integrity*, 20(6), 552–566.

Devine, T. (2015). *The corporate whistleblower's survival guide: A handbook for committing the truth*. Berrett-Koehler Publishers.

Executive Office of the President. (2021). *Executive Order 14028 on Improving the Nation's Cybersecurity*. Federal Register, 86(93), 26633–26647.

Federal Chief Information Officers Council. (2020). *Identity, Credential, and Access Management (ICAM) policy*. https://www.cio.gov

Greitzer, F. L., Kangas, L. J., Noonan, C. F., Brown, C. M., & Ferryman, T. A. (2012). Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats. In *2012 45th Hawaii International Conference on System Sciences* (pp. 2392–2401). IEEE.

Lind, E. A., Kanfer, R., & Earley, P. C. (2001). Voice, control, and procedural justice: Instrumental and noninstrumental concerns in fairness judgments. *Journal of Personality and Social Psychology*, 59(5), 952–959.

National Insider Threat Task Force (NITTF). (2020). *Insider threat program maturity framework*. https://www.dni.gov

O'Connor v. Ortega, 480 U.S. 709 (1987).

Office of the Director of National Intelligence (ODNI). (2012). *National Insider Threat Policy and Minimum Standards*. https://www.dni.gov

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). *Security in computing* (5th ed.). Pearson.

Reeves, M., & Whitaker, K. (2020). *The zero trust security playbook*. O'Reilly Media.

Relyea, H. C. (2008). The Privacy Act of 1974: A brief legislative history. *Government Information Quarterly*, 25(3), 370–376.

Shaw, E., & Sellers, L. (2015). Application of the Critical-Path Method to evaluate insider risks. *Studies in Intelligence*, 59(2), 1–11.

United States Government Accountability Office (GAO). (2018). *Cybersecurity: Agencies need to improve implementation of established policies and procedures*. https://www.gao.gov/products/gao-19-105

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.

Zetter, K. (2014). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Crown Publishing Group.