Journal of Recent Trends in Computer Science and Engineering (JRTCSE)
Volume 13, No.5, September - October, 2025, PP. 9-20.
ISSN: 2322-0872
https://jrtcse.com
DOI: https://doi.org/10.70589/JRTCSE.2025.13.5.2

Research Article

Insider Threat Management in Federal Workplaces: A Review of Technical and Policy Framework

Ahmad Ahmad*,
Masters in Cybersecurity and Information Assurance, College of Information Technology, Western Governors University, Salt Lake, Utah, USA.

Nurudeen Agbonoga,
Master of Science - MS in Computer Engineering, University of Texas at Dallas, USA

Abimbola Otun,
Master of Science - MS, Engineering/Industrial Management, Nottingham Trent University.

* Corresponding Author

Abstract

Insider threats remain one of the most persistent and damaging risks to national security, particularly in federal workplaces where access to sensitive information and critical systems is routine. These threats encompass both malicious insiders who intentionally exfiltrate data or sabotage operations, and unintentional actors whose negligence or error compromises security. Despite significant advancements in cybersecurity, insider incidents remain under-researched and under-mitigated, primarily due to the complexity of human behavior, organizational dynamics, and technological vulnerabilities. This article proposes a comprehensive framework for insider threat management that integrates advanced technical monitoring systems, artificial intelligence (AI)-driven analytics, and robust policy measures to safeguard federal workplaces. By combining lessons learned from high-profile incidents, current policy landscapes, and technological innovation, this framework offers a blueprint for federal agencies seeking to balance security, privacy, and operational efficiency.

Keywords: Insider Threat, Threat Management, Threat Landscape, National Security, Human Behavior.

Citation: Ahmad Ahmad, Nurudeen Agbonoga & Abimbola Otun. (2025). Insider Threat Management in Federal Workplaces: A Review of Technical and Policy Framework. *Journal of Recent Trends in Computer Science and Engineering, 13*(5), 9-20.
DOI: https://doi.org/10.70589/JRTCSE.2025.13.5.2

1. Introduction

The increasing pace of digital transformation in federal workplaces has ushered in unprecedented levels of efficiency, automation, and accessibility. Federal agencies are now deeply integrated with advanced information systems to manage sensitive operations ranging from national security and military intelligence to public health records, financial data, and citizen services. This rapid technological adoption has enabled federal systems to become more responsive to citizen needs, streamline bureaucratic processes, and enhance interagency collaboration. However, it has simultaneously introduced critical vulnerabilities, particularly in the form of insider threat risks originating from individuals within an organization who exploit their authorized access, either intentionally or inadvertently, to harm or compromise federal interests.

Insider threats are uniquely challenging because these individuals already possess legitimate access credentials and operational familiarity with sensitive systems. Unlike external adversaries, who must overcome perimeter defenses through cyberattacks or physical breaches, insiders can often bypass multiple layers of security with relative ease. The consequences of insider activity can be devastating, encompassing national security breaches, exposure of classified intelligence, erosion of public trust, financial losses, and long-term reputational damage for affected agencies. This highlights the importance of a comprehensive insider threat management strategy that strikes a balance between operational functionality and robust security oversight.

This work aims to explore the technical and behavioral dimensions of insider threats, emphasizing the intersection of evolving technologies, organizational dynamics, and human psychology; assess current U.S. federal and international policy frameworks, identifying successes, shortcomings, and lessons applicable across government and private-sector organizations; and propose a holistic, integrated framework for insider threat detection, prevention, and response that emphasizes scalability and adaptability for both large and small agencies.

By adopting this multidisciplinary perspective, this article will provide actionable insights for policymakers, security professionals, and federal leaders seeking to protect sensitive assets in an era of unprecedented digital connectivity and evolving insider threat landscapes.

2. Historical Perspective and High-Profile Cases

Insider threats are not simply a contemporary cybersecurity challenge; they are deeply rooted in the history of organizational risk, evolving from physical acts of espionage to complex digital breaches driven by modern technologies. Traditionally, insiders trusted employees or contractors posed threats through direct theft, sabotage, or espionage, often underpinned by ideological, financial, or personal motives. These incidents, although serious, were limited by the analog nature of information systems; data usually existed in tangible forms, such as paper. However, the digital transformation of the past

two decades, including shifts to cloud computing, remote work, mobile devices, and centralized data repositories, has dramatically expanded the scale, speed, and impact of insider threats (Mazzarolo & Jurcut, 2019; Sanyal et al., 2010).

This shift has magnified the consequences of insider activity. The most notorious examples, Edward Snowden and Chelsea Manning, serve as stark reminders of how privileged access and digital tools can enable individuals to inflict far greater harm than any physical intrusion ever could.

In 2013, Edward Snowden, working as a contractor for the National Security Agency (NSA), exfiltrated vast quantities of classified intelligence regarding global surveillance programs, dramatically altering public perception and international relations (Wired, 2013). Snowden's actions bypassed traditional perimeter security and highlighted the inherent vulnerabilities posed by trusted insiders with deep system access (Securonix, 2025). His case catalyzed a surge in insider threat research and forced both governmental and private organizations to scrutinize whether current defense systems adequately account for internal attackers (ASIS International, 2023).

Several years earlier, in 2010, Chelsea Manning, then a U.S. Army intelligence analyst, leaked hundreds of thousands of military and diplomatic communications to WikiLeaks. The leak revealed classified military operations, compromised informants, and strained diplomatic ties globally. Manning's insider act exposed the fragility of clearance-based access protocols, underlining the necessity for compartmentalization and behavioral monitoring (Mazzarolo & Jurcut, 2019).

Not all damaging insider incidents arise from intentional data theft. The Office of Personnel Management (OPM) breach in 2015 is a seminal example of how systemic weaknesses paired with inadequate security awareness can magnify the impact of external attacks. Although foreign threat actors were ultimately responsible for the breach, deficiencies in internal controls, such as poor encryption, outdated systems, and weak monitoring, played a significant role in enabling the exfiltration of over 21 million records containing sensitive personal and biometric data (Wired, 2015; Congressional Oversight, 2015; Wikipedia, 2025). Investigations revealed OPM had long been warned of these vulnerabilities but failed to implement necessary safeguards. This lapse manifested as one of the most damaging data breaches in U.S. federal history (Harvard Law Review, 2020).

Furthermore, unintentional insider threats stemming from employee negligence or exploitation via social engineering are increasingly consequential. Recent reports indicate that 83% of organizations experienced at least one insider incident in the past year, with negligent employees responsible for a substantial portion (Cybersecurity Insiders, 2024; Gurucul, 2024). One dataset revealed that negligent insider incidents cost organizations an average of $7.2 million annually, compared to $701,500 for malicious insider attacks. In comparison, broader data breach costs now average nearly $4.9 million (IBM/Ponemon Institute, 2025). These figures underscore the multiplicative risk that even non-malicious insiders pose when systems lack awareness and resilience.

Moreover, the exponential rise of generative AI is catalyzing a shift in the insider threat landscape. AI-powered tools are now enabling email impersonation, automation of credential misuse, and the creation of stealthy, authorized-looking insider behaviors, all executed at machine speed (ITPro, 2025; TechRadar, 2025). Despite these emerging challenges, only 44% of organizations currently use user and entity behavior analytics (UEBA) to monitor insider behaviors, a critical shortfall in modern detection postures (ITPro, 2025).

Reviewing these high-profile cases sets the stage for a pivotal realization: insider threats must be managed through a multidimensional lens. Foreign espionage, ideological whistleblowing, negligence, and external manipulation via social engineering all occupy different poles on the insider threat spectrum. This necessitates an integrated defense approach combining technical monitoring, behavioral analytics, policy modernization, and continuous education. In short, protecting critical federal systems demands more than perimeter defenses; it requires a proactive stance against varied, evolving internal risks.

2.1 Changing Threat Landscape in the Digital Era

The digital transformation of federal workplaces has significantly reshaped the cybersecurity landscape, introducing both enhanced capabilities and complex challenges. The integration of cloud-based systems, mobile devices, and remote or hybrid work models has expanded the attack surface, making traditional security perimeters increasingly obsolete. This evolution has given rise to a more sophisticated and multifaceted threat environment, where insider threats have become a primary concern for federal agencies.

Evolving Nature of Insider Threats

Insider threats, defined as security risks originating from within an organization, have evolved in both scope and complexity. Traditionally, these threats were primarily associated with malicious intent, such as espionage or sabotage. However, contemporary insider threats encompass a broader range of behaviors, including negligence, inadvertent errors, and compromised credentials. The motivations behind these threats are diverse, ranging from financial gain and ideological beliefs to personal grievances and unintentional mistakes.

A 2024 report by Cybersecurity Insiders revealed that 83% of organizations reported at least one insider attack in the previous year, with some experiencing multiple incidents. This statistic underscores the growing prevalence and severity of insider threats across various sectors, including federal agencies. The report also highlighted a significant increase in the frequency of insider attacks, with organizations experiencing five times the number of incidents compared to the previous year.

Challenges in Detection and Prevention

The detection and prevention of insider threats have become more challenging due to several factors. First, the adoption of cloud-based systems and mobile devices has

decentralized data access, making it difficult to monitor and control user activities effectively. Employees and contractors can access sensitive information from various locations and devices, often bypassing traditional security measures such as firewalls and intrusion detection systems.

Second, the shift to remote and hybrid work models has further complicated the detection of insider threats. Employees working from home or other remote locations may not be subject to the same level of oversight and monitoring as those working within the organization's physical premises. This lack of supervision increases the risk of malicious or negligent actions going undetected.

Moreover, conventional cybersecurity tools are often inadequate in identifying insider threats. These tools are primarily designed to detect external attacks and may not be effective in monitoring the activities of trusted insiders. As a result, insider threats can go unnoticed until significant damage has been done.

The Human Element in Cybersecurity

The human element has emerged as a critical factor in the evolving threat landscape. Behavioral patterns, organizational culture, and personnel vetting processes play a pivotal role in risk assessment and mitigation. Employees or contractors may act out of financial desperation, ideological motives, or personal grievances, while others may inadvertently introduce vulnerabilities by mishandling sensitive information or falling victim to sophisticated phishing campaigns.

Research indicates that human error remains a leading cause of cybersecurity incidents. A 2023 IBM Security report found that 95% of breaches are due to human mistakes, including falling for phishing emails, using weak passwords, and mishandling sensitive data. This statistic highlights the importance of incorporating the human factor into cybersecurity strategies.

Furthermore, organizational culture can influence the likelihood of insider threats. A culture that emphasizes security awareness, ethical behavior, and open communication can help mitigate risks by encouraging employees to report suspicious activities and adhere to security protocols. Conversely, a culture that downplays the importance of cybersecurity or discourages reporting can increase vulnerability to insider threats.

2.2 Federal and International Policy Context

Recognizing the severity of insider threats, the United States has implemented various frameworks to strengthen insider threat programs across federal agencies. Executive Orders such as EO 13587 (2011) established the requirement for agencies to develop insider threat detection and prevention strategies following the WikiLeaks disclosures. The creation of the National Insider Threat Task Force (NITTF) further institutionalized these efforts, providing guidance and best practices for federal entities to protect classified networks and information.

Globally, international partners have mirrored similar initiatives. For example, the United Kingdom's Centre for the Protection of National Infrastructure (CPNI) and Australia's Australian Security Intelligence Organisation (ASIO)have both prioritized insider threat management in their national security agendas. This international focus underscores the shared vulnerability faced by governments worldwide and highlights the need for collaborative sharing of threat intelligence.

Despite these advancements, gaps remain in implementation and integration, with many agencies struggling to strike a balance between operational privacy, employee trust, and necessary surveillance measures. This article aims to examine these challenges critically and propose a multilayered framework for addressing insider threats, combining technical, behavioral, and organizational strategies.

3. The Human–Technology Intersection

One of the most pressing complexities in insider threat management is the intersection between human behavior and technology. On the technology side, advanced analytics and artificial intelligence (AI) driven tools now enable security teams to monitor user behavior, detect anomalies, and flag potential risks in real-time. Yet, reliance on technology alone remains insufficient: insider threats are profoundly shaped by nuanced psychological, social, and organizational dynamics that cannot be fully captured through data analysis.

This intersection demands a holistic, integrated approach. Security teams must blend behavioral analysis with technical safeguards, conduct rigorous background checks and ongoing evaluations of employees in privileged roles, and cultivate a security-conscious workplace culture that emphasizes accountability without eroding employee morale.

3.1 Understanding Insider Threats

Definition and Categories. Insider threats refer to risks posed by individuals who have legitimate access to an organization's systems and data. As per NIST SP 800-53 and the NIST glossary, an insider threat involves any individual within the organization who uses their authorized access, either knowingly or unknowingly, to harm national security, organizational operations, or assets (NIST). The Cybersecurity and Infrastructure Security Agency (CISA) similarly defines insider threats as the potential for those with legitimate access, employees, contractors, or vendors, to intentionally or unintentionally harm mission-critical systems, data, or personnel (CISA).

Based on intent and behavior, insiders can be broadly categorized as:

Malicious insiders: Individuals who intentionally exploit their access for espionage, sabotage, or personal gain.

Negligent insiders: Employees who inadvertently cause harm due to carelessness, lack of training, or failure to follow policies.

Compromised insiders: Legitimate users whose credentials are stolen or manipulated by external actors to facilitate attacks.

These categories underscore the spectrum of insider threats, ranging from deliberate internal malfeasance to unintended consequences of poor practices or exploitation by adversaries.

Psychological and Organizational Drivers. Research shows that insider incidents often follow predictable psychological patterns. Common motivators include workplace dissatisfaction, financial stress, ideological beliefs, or a sense of grievance. When combined with technical gaps such as weak access controls or insufficient audit trails, these motivations can significantly elevate the risk of harmful actions.

Unique Federal Vulnerabilities. In federal workplaces, these risks are magnified. High-security-clearance roles, complex bureaucracies, and extended onboarding procedures create an environment ripe for exploitation. Without tailored detection and prevention mechanisms, federal agencies remain particularly vulnerable to both insider and blended insider–external threats.

3.2 Technical Controls in Insider Threat Detection

To combat insider threats effectively, federal agencies are increasingly deploying next-generation technological solutions. These include:

Behavior Analytics & Machine Learning

User and Entity Behavior Analytics (UEBA) and User Behavior Analytics (UBA) leverage AI and machine learning to model normal user activity and detect anomalies. These involve crafting behavioral baselines, tracking metrics like login patterns, data access volume, and application usage, and alerting when deviations occur.

Behavioral analytics frameworks, particularly those utilizing deep evidential clustering, have demonstrated high accuracy in real-world insider threat detection, achieving nearly 94.7% accuracy and reducing false positives by 38%.

Hybrid analytic models that combine unsupervised learning (e.g., clustering, autoencoders) with supervised approaches (e.g., classification models) are increasingly used to both detect novel threats and recognize known threat patterns.

Advanced architectures, such as LSTM neural networks, have also been explored for analyzing sequential user behaviors within logs to enhance the effectiveness of threat detection.

Zero-Trust Architectures & SIEM Integration

Zero-trust models require continuous authentication and assume that all users, even inside the network, could be potential threats. When coupled with behavior analysis, zero-trust ensures that each access request is continuously evaluated and assessed.

Security Information and Event Management (SIEM) platforms, often integrated with UBA/UEBA modules, allow centralized monitoring, log correlation, and incident response based on detected behavioral anomalies.

Behavioral Biometrics & Data Loss Prevention (DLP)

Behavioral biometrics, including keystroke dynamics, mouse movement, and voice recognition, offer an additional layer of authentication and real-time anomaly detection.

DLP systems automatically monitor, block, or flag unauthorized movement of sensitive data, helping prevent exfiltration.

All these systems work synergistically to detect insider threats through layered technical defenses.

Federal–System Specific Frameworks

Federally focused frameworks emphasize real-time anomaly detection, behavioral profiling, and low-latency response that align with regulatory mandates and mission-critical requirements.

Defense research programs such as DARPA's ADAMS and PRODIGAL projects leveraged graph analysis, machine learning, and statistical anomaly detection to identify insider threats via large-scale data mining, even at terabyte-per-day volumes.

3.3 The Human Factor: Limitations & Ethical Considerations

Despite the powerful capabilities of technical tools, over-reliance on surveillance can backfire:

Excessive monitoring can erode employee trust and morale, fostering suspicion and possibly driving covert, malicious behaviors. A case involving employee surveillance via microphone tracking without proper consent sparked legal action and highlighted how surveillance can harm trust rather than boost productivity.

Broader studies indicate that heightened monitoring, particularly among remote workers such as working mothers, increases stress and reduces workplace trust. This may lead to disengagement or concealment of risky behaviors.

Particularly in federal contexts, federal employees have expressed concerns that monitoring tools might be misused for political motives, undermining whistleblower protection and eroding legal safeguards.

These considerations underscore the importance of striking a delicate balance, ensuring security without compromising employee welfare or legal rights.

3.4 Integrated, Balanced Strategy

To address insider threats effectively, security leaders must implement an integrated approach combining technology, human factors, and organizational culture:

Technical Foundation

Deploy behavioral analytics, machine-learning-driven detection, zero-trust access controls, DLP, SIEM, and biometrics to monitor and detect potential insider threats continuously.

Personnel Vetting & Continuous Evaluation

Implement rigorous background checks, especially for privileged roles. Complement with ongoing screening and behavior evaluation to detect changes in risk profiles over time.

Culture & Trust

Promote transparency around monitoring practices. Provide clear communication regarding data collection methods, purposes, and safeguards to maintain employee trust.

Ethical Oversight & Policies

Develop and enforce governance frameworks that delineate ethical limits of surveillance, protect privacy, and comply with legal and regulatory requirements.

Training & Awareness

Offer regular training to help employees recognize signs of insider threats and phishing schemes, fostering a shared security responsibility mindset.

Incident Response & Forensics

Design incident response plans specific to insider threats. Conduct regular drills and ensure forensic data (logs, behavioral records) are captured and retrievable for investigation.

Continuous Improvement

Regularly review and refine detection models, policies, and training programs. Keep pace with evolving threats, emerging technologies (e.g., AI–driven insiders), and evolving regulatory norms.

4.0 Policy Landscape

Federal insider threat programs are primarily governed by directives, such as Executive Order 13587, which mandates the detection and prevention of insider threats within federal agencies. The Department of Defense (DoD) Insider Threat Program and the National Insider Threat Task Force (NITTF) have established best practices for risk assessment and personnel monitoring.

International frameworks, such as the EU's General Data Protection Regulation (GDPR), emphasize privacy-first approaches, creating tensions between security imperatives and employee rights. Striking this balance is a recurring challenge. Policies must clearly define the limits of surveillance, ensure due process for employees flagged as high-risk, and include whistleblower protections to prevent retaliation.

4.1 Proposed Technical and Policy Framework

The proposed insider threat framework is built on two pillars:

Technical Layer: AI-driven analytics, multi-factor authentication, zero-trust models, and endpoint detection systems form the core of a technical defense strategy. Advanced

anomaly detection should leverage ML algorithms trained on historical insider threat data.

Policy Layer: Continuous workforce vetting, mental health support programs, and clear communication of security policies foster an environment of transparency and accountability. Federal agencies should implement periodic clearance renewal, mandatory cybersecurity training, and psychological wellness check-ins to identify early warning signs.

4.2 Case Studies

Edward Snowden (2013): Snowden's ability to access and exfiltrate classified NSA data illustrates systemic weaknesses in privileged access management and insider monitoring.
Chelsea Manning (2010): Overly permissive access policies allowed the mass extraction of classified military data.

OPM Breach (2015): Although primarily a result of external threat actors, internal negligence and outdated systems played critical roles in facilitating the attack.

5.0 Challenges and Ethical Considerations

Implementing robust insider threat programs within federal agencies introduces significant ethical, legal, and organizational complexities. While these programs aim to secure sensitive data and infrastructure, their design and execution can inadvertently impact employee rights, trust, and fairness. A balanced framework requires careful attention to oversight, privacy, bias, and whistleblower protection.

5.1 Privacy and Workplace Morale

Employee Privacy: Insider threat programs often involve extensive monitoring, tracking communications, digital behavior, access logs, and metadata. Such surveillance can erode expectations of privacy and create a workplace culture of suspicion. Surveillance without clear limits or transparency may feel invasive, especially when employees are unaware of the extent or purpose of monitoring.

Morale Risks: Excessive surveillance can stifle morale, inhibit collaboration, and create anxiety among employees. Federal workers have expressed concerns that monitoring tools could be misused for political or disciplinary purposes, thereby undermining trust in leadership and discouraging open communication. For instance, federal employees expressed fear that insider threat systems could be weaponized to suppress dissent or whistleblowing, particularly under politically charged leadership transitions.

5.2 Algorithmic Bias and Fairness

Bias in AI Tools: Many insider threat programs rely on AI and machine learning to flag anomalous behavior. Without careful design and oversight, these systems may reflect or reinforce biases flagging innocent employees more frequently due to attributes unrelated to threat (such as job role, schedule, or demographic characteristics).

Ethical Auditing: To mitigate bias, organizations should adopt ethics-based auditing methodologies that structure evaluations that assess algorithmic decisions against norms of fairness, transparency, and accountability. These audits help identify discriminatory patterns and ensure that automated decisions align with institutional values and legal standards.arXiv

5.3 Oversight Committees

Purpose of Oversight: Oversight committees play a critical role in ensuring that insider threat programs remain ethical, effective, and legally compliant. These bodies typically include representatives from departments such as Privacy, Civil Rights, Human Capital, Counterintelligence, Legal, and others.

Examples in Practice: Legislative text establishing Insider Threat Steering Committees composed of Under Secretaries, Chief Security Officers, Office of General Counsel, Privacy Office, and more mandates regular meetings to align insider threat operations with policy, legal oversight, and whistleblower protections. Such oversight ensures policies are holistically developed and non-discriminatory.

5.4 Privacy Impact Assessments (PIAs)

Assessing Program Impact: Before deploying surveillance tools or behavioral analytics, agencies should conduct Privacy Impact Assessments to evaluate how data is collected, stored, used, and protected. PIAs help identify privacy risks and inform mitigations such as limiting data retention, anonymization, or transparency to stakeholders.

Independent Review: Ideally, PIAs should undergo independent review (e.g., via the Privacy and Civil Liberties Oversight Board, PCLOB) to ensure civil liberties are preserved. The PCLOB, established in 2004, advises the executive branch to balance security strategies with privacy and civil liberties.

6.0 Conclusion and Future Directions

Federal workplaces represent a high-value target for insider threats, necessitating a multi-layered defense strategy. By combining technical innovation with transparent policy frameworks, agencies can better detect, prevent, and respond to insider incidents. This article's framework provides a foundation for future research and implementation, emphasizing that insider threat mitigation is as much a human challenge as it is a technological one.

Future insider threat management should emphasize predictive analytics, organizational psychology, and interdisciplinary collaboration. The integration of AI with psychological risk profiling may enable real-time intervention before harmful incidents occur. Agencies should also invest in gamified employee training and red-team simulations to improve organizational preparedness.

References

ASIS International. (2023, April 17). The state of insider threat initiatives 10 years after Snowden. Security Management Magazine. ASIS International

Cybersecurity Insiders. (2024). 2024 Insider Threat Report. GuruculIBM

Gurucul. (2024, October 23). Understanding the risks and mitigation of insider threats. Gurucul

Harvard Law Review. (2020, Jan 10). In re U.S. Office of Personnel Management data security breach litigation. Harvard Law Review

IBM / Ponemon Institute. (2025). Cost of a Data Breach Report 2025. IBMTeramind -

ITPro. (2025). AI means cyber teams are rethinking their approach to insider threats. IT Pro

Mazzarolo, G., & Jurcut, A. D. (2019). Insider threats in Cyber Security: The enemy within the gates. arXiv. arXiv

Sanyal, S., Shelat, A., & Gupta, A. (2010). New frontiers of network security: The threat within. arXiv. arXiv

Securonix. (2025). Edward Snowden – The Ultimate Insider Threat. Securonix

TechRadar. (2025). AI set to supercharge insider threats. TechRadar

Wired. (2013). NSA whistleblower: The ultimate insider attack. WIRED

Wired. (2015). Why the OPM breach is such a security and privacy debacle. WIRED

Wired. (2016). Inside the cyberattack that shocked the US government. WIRED

Wikipedia. (2025). Office of Personnel Management data breach.