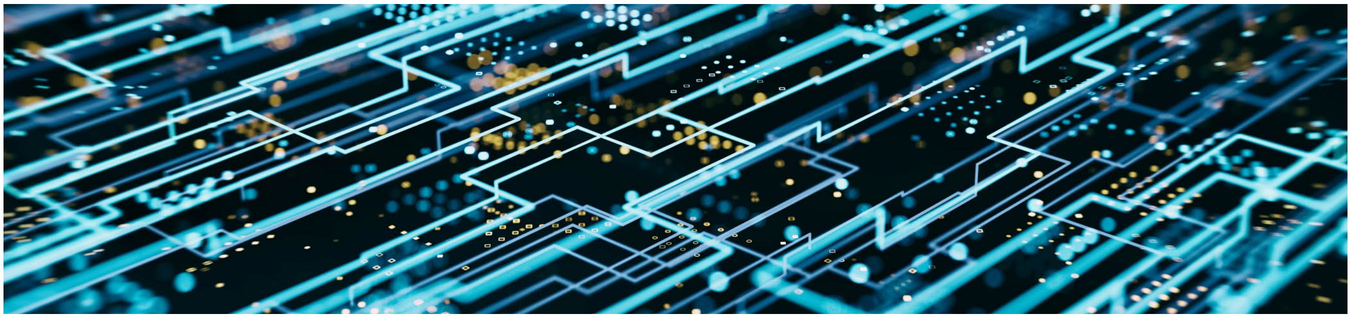
Best Practices for and Dispelling Myths Surrounding Modern Insider Threat Programs

Structural and Policy Drivers Necessary to Protect Information and Systems



Grant Schneider
Senior Director of Cybersecurity Services

Ross B. Nodurft
Senior Director of Cybersecurity Services

Elizabeth Guillot
Cybersecurity Policy Analyst

September 20, 2021

In Collaboration with Forcepoint

VENABLE LLP

Scene Setter

Imagine getting a call from your insider threat team alerting you that an employee has created a target list of current and former elected officials whom he would like to harm. Adding to the severity of the situation, that same employee recently purchased illegal drugs and weapons and spent hours reading manifestos of mass murderers on his government computer. While this may sound too dramatic to be true, in 2019 a U.S. Coast Guard lieutenant created such a target list and purchased illegal drugs and weapons and much more before he was caught and arrested because of an insider threat program.[1]

Unfortunately, when employers fail to notice warning signs, insider threats are not detected and may result in major damage to both people and organizations. Missed insider threats can have a wide range of results, from a person knowingly or unknowingly releasing data or even individuals harming themselves or others. Understanding and detecting insider threats is a balancing act, as most employees have positive intentions and serve as every organization's greatest resource. However, people are imperfect, and they are one of the greatest sources of risk to an organization. People make mistakes; they miss critical information; and on rare occasions, they deliberately seek to damage or undermine their organization. This delicate balance is just one of the reasons organizations need a holistic program to make sure employees are on the right path, without violating the trust between employee and employer.

In light of recent high-profile ransomware attacks, and attacks on federal government networks, cybersecurity and data security are on the minds of government and business leaders alike. To address and provide guidance on cybersecurity issues, the Biden administration released Executive Order 14028, Improving the Nation's Cybersecurity in May 2021.[2] This executive order focuses on improving the federal government's cybersecurity by modernizing practices and increasing the security requirements for vendors to the federal government. While many of the implementation policies for Executive Order 14028 are still forthcoming, the Biden administration has recognized that organizations are more dependent on technology for every aspect of their operation than ever before.

In today's technologically advanced business world, our sensitive information is electronically collected and stored; our workflows are captured and processed in automated systems; and intellectual property is carefully watched. The recent widespread adoption of working from home by many organizations due to COVID-19 has also introduced new challenges. As employees are working from home, an organization loses many opportunities to physically notice troubling behavior. An organization also misses many of the digital touchpoints with employees as personal devices begin to double as a work device. This leaves room for an insider threat to go undetected without a proper program in place. Domestic terrorism, like the example described above, is a persistent problem facing the U.S. This growing threat adds another layer companies and agencies must be on the lookout for, and detecting this behavior is more difficult in the changing work environment.[3]

[1] https://www.cdse.edu/documents/cdse/case-study-paul-hasson.pdf

[2] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[3] https://www.whitehouse.gov/wp-content/uploads/2021/06/National-Strategy-for-Countering-Domestic-Terrorism.pdf

Executive Summary

Agency heads are responsible for taking a risk management approach to protecting their systems, data, and personnel. As such, they have the authority and flexibility to implement appropriate security controls to protect their organizations. A comprehensive insider threat program is an important part of any organization's security portfolio. It is especially important for government agencies, as they house sensitive and classified information.[4] Insider threat programs can also be very effective at stopping employees at risk of harming themselves, others, or the organization. Although the effectiveness of insider threat programs has been demonstrated in multiple cases, there is no clear policy guidance on the implementation of such programs outside of classified networks. Only one policy directive mandates insider threat programs on classified networks for U.S. government agencies, and it does not address monitoring on unclassified networks. However, other government reports reference insider threat programs on all networks as a best practice.

User Activity Monitoring, or UAM, is an essential tool for any insider threat program. While in practice the tool can protect employees' privacy and save the organization money, there are misconceptions about UAM. There are also misunderstandings that UAM should only be used on classified networks or only involve IT staff—which could not be further from the truth. UAM is most effective when used on both classified and unclassified networks and when various departments such as HR, IT, physical security, legal, and management are all involved in the program.

As organizations implement insider threat programs, there are best practices that can be applied to organizations of all sizes. If an organization uses the National Institute of Science and Technology (NIST) Cybersecurity Framework[5] (the Framework), many of the Framework elements can be satisfied by an insider threat program.

Additionally, it is important that various departments play a role in reporting to the program and in responding to emerging threats or incidents. Since working from home has increased drastically, it is important for programs to monitor both person and non-person endpoints to have a fuller picture of the network. An insider threat program can also be tailored specifically for an organization's needs and requirements. It is an upfront investment to implement an insider threat and UAM program, but it can save costs, both monetary and reputational, in the long run. Thus we have included five key recommendations for both policy makers and practitioners with regard to the implementation of such programs:

1. Mandate and provide clear policy guidance for insider threat and UAM programs across all networks and individuals regardless of clearance status;
2. Educate decision makers on UAM programs to prevent misperceptions about the technology;
3. Drive collaboration across departments within organizations to enable an effective insider threat program;
4. Leverage UAM capabilities to protect against threats to physical, cyber, and information security; and
5. Empower agencies through policy and resourcing to build insider threat programs and use tools like UAM.

These recommendations flow from a robust review of the current federal government policy landscape and a series of interviews conducted with security, technology, and administration professionals from public and private sector companies. While threats exist across private companies and government agencies alike, this paper focuses on the unique situation many government agencies find themselves in as they look to implement or follow guidance on insider threat programs.

[4] Sensitive information can include unclassified information, information held by human resources, business information, personal health information (PHI), etc.

[5] https://www.nist.gov/cyberframework

The Current Policy Landscape

There are many policies[6] that provide guidance for protecting federal information and systems from threats impacting the confidentiality, integrity, or availability of that information. These policies direct agencies to take a risk management approach to cybersecurity, while providing the authority to implement necessary protections, including insider threat programs on unclassified networks. However, most of the policies fail to explicitly mention insider threat programs. The one exception is Executive Order (EO) 13587, which mandates insider threat programs for classified environments; however, it provides no direction for unclassified systems. This leaves agencies confused as to what steps they need to take to protect their unclassified systems from insider threats. Some agencies interpret EO 13587 to mandate that UAM must be maintained for all individuals who hold a security clearance and have access to classified systems, regardless of which system they are operating on. Other agencies interpret the guidance to mean that use of UAM is required only while users are logged into and using their accounts on classified systems. Meanwhile, another group of agencies has decided that UAM is allowed and appropriate for all users on all accounts. These differences in interpretation create inconsistencies in the government's approach to insider threats. Inconsistencies in addressing insider threats ultimately provide opportunities for malicious insiders, as well as accidental insiders, to exploit vulnerabilities across key systems, leading to exposure of sensitive data or other types of damage.

Below we have highlighted some of the most relevant policies that agencies must comply with in this space.[7]

- **EO 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information:** EO 13587 provides the only policy direction for insider threats and sets the stage for insider threat programs within federal classified networks. The EO was a response to the disclosure of classified information to WikiLeaks by an insider[8] and requires implementation of an insider threat detection and prevention program on classified networks.[9] It also created the National Insider Threat Task Force, which has developed policies and priorities for establishing insider threat programs.

- **National Insider Threat Task Force (NITTF) reports:** NITTF released a guide in 2017 recognizing that many agencies house information that is extremely sensitive on unclassified networks. The guide recognized that standards for classified networks can also be applied to protect sensitive unclassified networks.[10] In 2018, NITTF published an additional document, *Insider Threat Maturity Framework*, as an aid to federal agency programs wanting to go beyond the minimum standards. One of the maturity principles calls for the establishment of UAM on all U.S. government endpoints, devices, and government-owned IT resources connected to U.S. government computer networks.[11]

- **NIST's Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations (NIST 800-53):** NIST 800-53 includes insider threat controls in sections discussing awareness and training, incident response, and program management. Federal agencies are required to comply with NIST 800-53. NIST 800-53 requires that an insider threat program include a cross-discipline insider threat incident handling team, including human resources, personnel offices, physical security, and legal counsel. NIST 800-53 also offers some control enhancements regarding insider threat programs.[12]

[6] Laws, executive orders, memorandums, regulations, strategies, and other types of guidance.

[7] See Appendix A for more details.

[8] https://www.bbc.com/news/10255887

[9] https://obamawhitehouse.archives.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net

[10] https://www.dni.gov/files/NCSC/documents/nittf/NITTF-Insider-Threat-Guide-2017.pdf

[11] https://www.dni.gov/files/NCSC/documents/nittf/20181024_NITTF_MaturityFramework_web.pdf

[12] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf#page=463&zoom=100,117,96

- **Committee on National Security Systems Directive 504 – Directive on Protecting National Security Systems (NSS) for Insider Threat:** The directive requires that UAM be implemented on all national security systems, both classified and unclassified, that contain information related to weapons systems and/or military operations.

- **EO 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure:** EO 13800 directs that each agency head use the Framework for Improving Critical Infrastructure Cybersecurity (the Framework), developed by the National Institute of Standards and Technology (NIST), or any successor document to manage the agency's cybersecurity risk. The Framework serves as a guide for organizations of all sizes, in all sectors, to examine how they are managing their cybersecurity risk but does not provide any specific guidance with respect to insider threats.[13]

- **Federal Information Security Management Act of 2002 (FISMA) and its update, Federal Information Security Modernization Act, in 2014:** FISMA directs agencies to protect federal information and systems from potential harm and compromise. It also requires that agencies comply with federal standards, guidance, and policies related to federal information security; however, it has no requirements with respect to insider threats.[14]

- **Personnel and technology policies:** Government agencies also have personnel policies and policies for behavior on government devices that are specific to the agency. While these personnel and technical policies are important, inasmuch as they state the rules and let employees know what is and is not allowed without any type of monitoring program, neither unintentional mistakes nor malicious behavior can be detected.

While it is important to protect classified networks with the best technology available, insider threats are not limited to classified networks. As we can see from the policies listed above, the government does not require insider threat programs for unclassified networks. Guidelines such as NITTF's *Insider Threat Maturity Framework* make it clear that agencies looking to take the next step in protecting their data and networks should be monitoring not only classified networks but unclassified as well, to increase the chances of finding an insider threat. However, these are guidelines, not requirements.

[13] https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure

[14] https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

User Activity Monitoring: Myth vs. Fact

Policy makers recognize that threats exist on both classified and unclassified networks, but existing policies do not reflect that fact. In discussions with policy makers, Venable found that the concept of expanding UAM on unclassified networks frequently leads to questions about privacy, scope, and cost. In this section, we discuss common myths that often arise in discussions with both policy makers and operational executives about UAM on unclassified networks.

UAM is a capability that allows organizations to track user action on devices that belong to the employer. Organizations use these tools to detect, stop, and intervene when an insider threat arises. UAM programs are effective in stopping both malicious actors and unintentional mistakes. Given the nature of UAM software and programs, it is unsurprising that people have questions, and often misunderstandings, about how monitoring works, what networks it should be used on, and how to address privacy concerns. However, with full transparency on how UAM programs operate, many reservations should be resolved.

Myth #1 – Insider threats exist only on classified networks

As discussed in the policy overview section, the only policy mandating insider threat programs focuses solely on classified networks. While it is understandable to conclude that monitoring activity on classified networks is most important since that is where the most sensitive information is stored, there are three key reasons why this approach is not sufficient to protect an organization and its assets.

First, unclassified networks contain a large amount of very sensitive information that could cause significant harm if it were to be improperly disclosed. As departments, agencies, and service branches move more of their unclassified missions to virtual environments, the amount of sensitive information on unclassified networks continues to grow.[15] Employees also often have remote access to their organization's unclassified network and to the sensitive information on that network. Focusing on user activities that occur exclusively on classified networks ignores issues related to data that is readily available on unclassified networks, data that can be highly sensitive both alone and in the aggregate.

Second, there are clear physical, technical, and social cues that restrict the potential range of risky activities users can perform on classified networks. When users are logged into a classified network, they are typically in the office, where they can be observed and have passed through one or more physical security checkpoints. Classified networks often have additional security banners that constantly remind users that they are on a sensitive system. Additionally, users' activities are limited by the content available on such networks, content that is typically limited to work-related materials. While UAM is still important in these environments, the scope of activities is restricted by network controls.

Third, user activity on unclassified networks provides insights into an individual's intent. Certain types of human threats, such as employees who want to cause harm to themselves or others, are more likely to be detected on unclassified networks where the users have free access to internet content and expanded ability to communicate with whomever they choose via a range of communication channels. Unclassified networks provide an ideal environment for understanding user behaviors and activities because there are fewer constraints, and behaviors are not artificially shaped by boundaries found on classified networks.

In further support of this concept, the National Counterintelligence and Security Center's recent publication, *Insider Threat Mitigation for U.S. Critical Infrastructure*, notes that there is an inclination to believe that UAM only needs to be on an organization's most sensitive networks, but human behavior on open networks can better indicate a problem.[16]

[15] https://www.fedscoop.com/list/7-federal-agencies-making-telework-now-beyond/

[16] https://www.dni.gov/files/NCSC/documents/nittf/20210319-Insider-Threat-Mitigation-for-US-Critical-Infrastru-March-2021.pdf

Deploying a UAM program on unclassified networks can also curtail unwanted behavior on a classified network. Individuals are more likely to start showing trends of bad behavior on the unclassified network before they would on the classified network. For example, unclassified network monitoring can provide earlier indicators of bad behavior, such as workplace bullying, threats or risk of self-harm, and disgruntlement, that would not likely be identified via classified network monitoring. Early identification also enables organizations to address such behavioral issues before they reach classified networks.

Myth #2 – UAM programs "spy" on employees

The idea of being tracked or watched while at work can be understandably concerning for many individuals. Most employees admit to online shopping at work,[17] checking personal email addresses, or visiting social media sites. The result is that UAM programs can feel like they infringe upon personal matters employees manage while working. However, UAM programs are important tools for detecting insider threats and are about protecting both employees and organizations. These capabilities can make it possible to recognize when an employee's credentials have been compromised. An ethically configured UAM program gathers information to find trends rather than looking at employees' every move on their computer. It is likely that your employer does not care if you are checking Facebook; however, your employer would care if you're downloading the full contents of a department's shared folder and uploading it to personal accounts or sharing with recipients outside of your organization.

The settings of a UAM system are customizable and allow organizations to tailor what is and is not monitored. For the average organization, legal departments and human resources departments review these settings to ensure there are no infringements on employees' privacy. The typical UAM program works by collecting information within the bounds of the pre-approved settings and sends that data into the UAM system. The program takes in a lot of information, but the majority of that data is never analyzed, used, or seen by a human.

Rather, it is stored for a period of time in case an incident does arise. Additionally, the information collected by the UAM program can be anonymized to protect employees' privacy. Policies put in place by the organization create rules for when to flag actions for human review. For the most part, these policies look for potential harm to other employees, harm to self, or harm to the organization. UAM programs are not looking at every action an employee takes, but rather are looking at big picture trends so they are able to spot an action that is out of character.

This is not to say that organizations with insider threat programs do not trust that employees will act in good faith, but rather they recognize that in today's fast-paced work environments, employees are likely to make occasional mistakes, and there are unfortunately rare bad actors.

Myth #3 – UAM programs are not worth the investment

Security of an organization—both physical and digital—is a cost center, not a profit center. It can be hard to justify increasing budgets for a new program or technology when it will not bring in money. A budget sheet of a company has only money in and money out; it does not have a column for "money that was stopped from being lost."

Establishing UAM capabilities requires investment of both time and money. However, this investment can pay off tenfold if even one insider threat is prevented. While difficult to enumerate because of the wide range of outcomes linked to insider threat events, there are significant monetary costs for liabilities and reputational damage caused by data leaks, system sabotage, and acts of violence. For example, Equifax stated that the company spent $1.4 billion to improve its network and data security after the attack, and in a settlement with the FTC it was required to pay $1.38 billion to consumers whose data was leaked.[18] While Equifax was one of the most expensive data breaches to date, IBM's *Cost of a Data Breach Report* 2020 found that the United States has the most

[17] https://www.fastcompany.com/90408181/you-shop-online-at-work-we-all-know-it-and-this-research-proves-it

[18] https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

expensive data breaches—averaging $8.64 million per breach.[19] An organization of any size can be subject to harsh consequences in the event of a data breach.

Measuring the impact of insider threat incidents on reputation is extraordinarily challenging, and while stock prices provide one value for assessing the reputation of publicly traded companies, for private companies the impact is more difficult to understand. That said, regardless of the metrics used for understanding the impact of events such as a data breach, costs associated with such events are often unplanned and more expensive than expected. Unanticipated expenses can disrupt organizations of all sizes and can ultimately disrupt supply chains and resources for the broader population. Reputational costs, and the inability to perform critical organizational functions because of lost revenue or unplanned expenses, are very serious and far outweigh the immediate cost of implementing a new technology.

Customer Feedback

Venable interviewed government customers and non-customers of UAM capabilities to gather information. From interviews, we found the following:

- Organizations using UAM tools reported significantly shorter timelines to close investigations.
- There is confusion over UAM policies and the authority of government agencies to implement UAM tools on unclassified networks.
- UAM programs save money over time.
- Privacy concerns can be mitigated through UAM settings and legal department guidance.

A comprehensive insider threat program that utilizes UAM can also save both time and personnel costs. UAM programs that use algorithms and machine learning to build user profile baselines can reduce the number of staff needed to review insider threat program information or reduce staff workload so they can focus on high-level alerts that require human judgment. A UAM program can quickly examine what times an individual usually works or what files are used; in contrast, that could take a human an hour to do when his or her time could be better spent examining an escalated case. Insider threat programs can also be used to help retain employees by flagging those who are starting to show signs of unhappiness, if an organization chooses to utilize this type of feature. Instead of a company having to hire and train a new employee, a UAM could have anonymized settings to flag an employee who is being underutilized or who is using language that demonstrates disgruntlement. With this information, HR or another appropriate department could take steps to increase employee satisfaction.

Myth #4 – Insider threat programs only involve IT department staff

Some organizations view insider threat as a part of their overall cybersecurity programs. In this context they see insider threats as being only about data loss prevention and run their program in a silo within the IT or network security organization. A strong insider threat program includes participation from various parts of an organization. Physical security can gather intelligence on how people behave when they are not online. IT and network security can administer a UAM program and make sure it is appropriately carried out. Human resources can provide both critical information on performance reviews and notes from managers in addition to making sure employees' private information is kept safe. Analysts can look at any information that is brought to their attention and make recommendations on different courses of action. Counterintelligence can look for signs that an insider has been compromised by an enemy. Leadership and the legal department set the boundaries for any program to ensure both the organization and individuals are adequately protected. All of the roles laid out can produce valuable information, but unless all of these different facets are working together and sharing information, it is impossible for an organization to get a full picture of a potential insider threat. Figure 1 is a diagram of the departments that typically have a role to play in an insider threat program and the horizontal nature of their involvement.

[19] https://www.ibm.com/security/data-breach

In addition to various departments playing an important role in the collection of information for a successful insider threat program, they also have a role to play if an insider threat is identified. The correct person in an organization dealing with a threat can be the difference between the threat being resolved positively or an issue taking a turn for the worse. For example, if the identified individual could harm others, physical security might be the correct personnel to deal with the threat; or if someone is at risk of harming themselves, human resources might be the best department to help that person. If the IT department is the only team involved in an insider threat program, it could put IT professionals in a position where they are dealing with sensitive situations without the necessary training—putting both the IT professional and insider threat at risk.

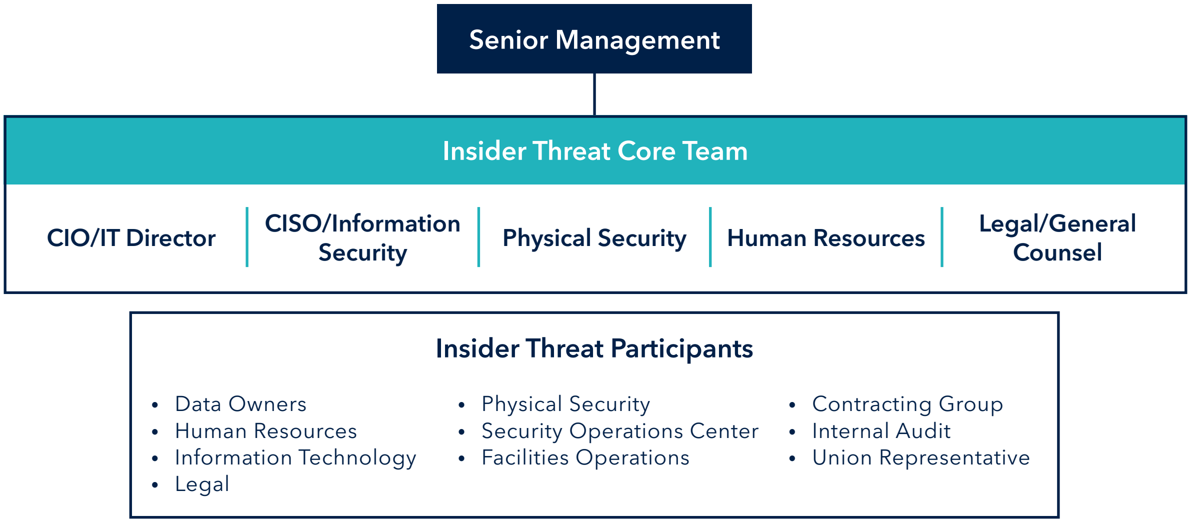


Figure 1

Best Practices

As policy makers consider issuing directions to departments, agencies, and service branches, best practices should be considered during deployment of insider threat and UAM programs.

Alignment with NIST Cybersecurity Framework

The NIST Cybersecurity Framework has become widely adopted because of its risk-based approach and collaboration with industry stakeholders. Many elements of the Framework's principles can be achieved by implementing an insider threat program. For example, the Framework calls for information, records, and data to be managed in a way that is "consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information."[20] An insider threat program can ensure that all data, both classified and unclassified, is protected from threats within an organization. Another principle outlined by the Framework calls for anomalous activity to be detected.[21] Detecting anomalies and events out of the ordinary is one of the most effective features of UAM since it identifies a baseline of normal behavior and then can detect behaviors out of the ordinary. Finally, the Framework calls for continuous security monitoring; this principle can be applied to security monitoring for both external and internal threats.

In addition to fulfilling specific principles of the Framework, an insider threat program aligns with the spirit of the document. Organizations that deal with classified or sensitive information have higher risk because 1) bad actors are constantly after sensitive information; and 2) there are greater consequences for the organization if sensitive information is leaked. Taking a risk-based approach, the higher the risk, the more steps and layers of security are needed to protect the sensitive information and organization at large. An insider threat program is a step that organizations can take beyond baseline security requirements to make sure information is secure.

Collaboration Across Various Stakeholders

As the dispelled Myth #4 and Figure 1 describe, many different parts of an organization play an important role in managing an effective and holistic insider threat program. It is critically important for senior leadership to champion the program and assign a senior accountable official to lead the effort. That official is then charged with ensuring IT departments, physical security officers, legal departments, human resources, and employee managers all understand their roles in the insider threat program and understand what their reporting duties are. It is equally important that these various departments then communicate with each other. Another key stakeholder is the workforce. Dispelled Myth #2 points out that an insider threat program is not about spying on individual employees. However, this must be regularly emphasized by communicating the scope and objectives of the insider threat program to employees. A centralized insider threat program takes in various bits of information across the organization and then raises the appropriate flags if there is an issue. A disjointed program cannot be effective.

A prepared incident response plan that includes all stakeholders is another element of collaboration that should not be overlooked. An organization's response to a potential data theft is very different from the response to a potentially violent individual. In addition to making sure key stakeholders are aware of their reporting duties, employees should be aware of a role they could play once a threat is identified. For example, who authorizes IT to terminate an employee's access to the network, or when does Human Resources intervene with an employee showing signs of distress? The individual who is leading the implementation of an insider threat program must ensure an incident response plan is part of the effort.

[20] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[21] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Alignment with Zero Trust Architectures

Executive Order 14028, Improving the Nation's Cybersecurity (Cybersecurity EO), makes it clear that new technologies and methods should be embraced to bolster overall cybersecurity, and agencies must adopt zero trust architectures.[22] Zero trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated.[23] In order to implement a zero trust architecture and continually evaluate trust, agencies must implement an insider threat program. An insider threat program, including a UAM program, allows organizations to know what users are doing as a key part of the continuous evaluation in a zero trust architecture. A UAM program can also help establish a baseline of behavior for users, so that behavior that is out of the ordinary can be detected through zero trust principles. Zero trust also requires organizations to shift from the traditional thinking of network-based security to security focusing on users, assets, and resources.[24] UAM is that next step in defense beyond network security, because it focuses on user activity and access to data. It can also help with authenticating users. Agencies working to implement the zero trust requirement of the Cybersecurity EO should use an insider threat program and UAM programs to meet the requirements.

Monitoring Person and Non-Person Endpoints

As an organization is setting up UAM as part of an insider threat program, it might seem that it is enough to monitor only individuals on that organization's network. However, as work from home has increased exponentially in the last year, it is more important than ever to also incorporate non-person endpoints into a UAM strategy. Monitoring individuals is an effective strategy if every person is in the office, on the same device each day, and on the same network, but not many workplaces currently operate under that structure. Today, many employees use a mixture of company-issued and personally owned devices for work, including laptops, tablets, and cell phones, all of which could be vulnerable to an attack. As more attacks are caused by bad actors gaining access through endpoints instead of networks, it is important for UAM, and insider threat programs in general, to consider the changing work dynamic ushered in during the pandemic.

[22] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[23] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[24] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Key Recommendations

Cybersecurity attacks are increasing across all industries and government. Organizations can no longer be passive with their cybersecurity and need to take proactive steps to protect themselves from future attacks. As part of a zero trust architecture, building a robust insider threat program can help organizations identify and prevent cyberattacks, along with physical attacks. Embracing technologies such as UAM in an insider threat program increases the ability to catch bad actors and boosts overall security.

Below is a series of recommendations that stem from discussions with policy and operational professionals in both government and industry, in addition to a robust review of the current government policy landscape.

Key Recommendation #1: Mandate and provide clear policy guidance for insider threat and UAM programs across all networks and individuals, regardless of clearance status.
While insider threat and UAM programs have proved effective in many different use cases, there is inadequate coverage of insider threat protections for unclassified systems and information. The executive branch should provide clear and comprehensive guidance directing the implementation of insider threat and UAM programs across all networks to enable a holistic assessment of people, protected assets, and sensitive data

Key Recommendation #2: Educate decision makers on UAM programs to prevent misperceptions about the technology.
There are many myths surrounding UAM programs, as discussed above. Proper education about what a UAM program is and how it directly supports an organization mission is critical. Decision makers need to understand the business value of a UAM program and how it can be implemented to protect employee privacy through anonymization and collection policies.

Key Recommendation #3: Drive collaboration across departments within organizations to enable an effective insider threat program.
Collaboration and involvement by many different departments is important to building a fruitful insider threat program. IT, human resources, legal, physical security, and management all have a role to play in the input of data and response to an incident. Having a full picture of an actor who presents a potential threat—including their online and physical actions—is important for measuring the risk level of a situation. When an insider threat is identified, the department that should lead the response depends on the type of risk the individual presents.

Key Recommendation #4: Leverage UAM capabilities to protect against threats to physical, cyber, and information security.
Deploying UAM across all networks and users provides capabilities to protect against threats to information systems, data, facilities, and the workforce. As we saw in Myth #4, UAM capabilities can help an organization do more that prevent data loss. When properly used, these capabilities can help identify and prevent insiders who seek to harm themselves or others through some form of domestic terrorism.

Key Recommendation #5: Empower agencies through policy and resourcing to build insider threat programs and use tools like UAM.
Agencies are currently uncertain of what their authorities and obligations are with respect to insider threat and UAM programs. In addition to adding clarity under Key Recommendation #1, agencies must be adequately funded to implement these programs to protect sensitive, classified, and other government information.

Appendix A

Name	Requires Insider Threat Program?
Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information	**Yes** EO 13587 provides the only policy direction for insider threats and sets the stage for insider threat programs within federal classified networks. The EO was written as a response to the Wikileaks incident in 2010 involving the release of thousands of State Department cables, which had been removed from a classified network by a malicious insider. Given the nature of the compromise, the EO was written to address insider threats to classified networks and does not address unclassified systems. The executive order requires implementation of an insider threat detection and prevention program on classified networks. It also creates the National Insider Threat Task Force, which has developed policies and priorities for establishing insider threat programs.
The National Insider Threat Task Force (NITTF) guides	**Yes** The National Insider Threat Task Force (NITTF) released a guide in 2017 that recognizes many agencies house information that is extremely sensitive and critical on unclassified networks. The guide states that all of the policy and standards the NITTF has published for classified networks can also be applied to protect sensitive unclassified networks. In 2018, NITTF published an additional document titled Insider Threat Maturity Framework as an aid to federal agency programs wanting to go beyond the minimum standards. One of the maturity principles is establishing UAM on all U.S. government endpoints, devices, and government-owned IT resources connected to U.S. government computer networks. It goes on to recommend that agencies look at monitoring all assets, regardless of whether they are classified or unclassified, that could cause damage if compromised.
NIST Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations	**Yes** The updated version of NIST's Special Publication 800-53 includes insider threat controls as part of the awareness and training family of controls, along with the incident response and program management control families. Federal agencies are required to comply with NIST 800-53, and Executive Order 13587 is referenced as creating the requirement for insider threat monitoring on classified networks. NIST 800-53 insider threat program control requires that an insider threat program include a cross-disciplinary team. Insider threat programs are discussed again in the incident-handling control, which requires a coordinated incident-handling capability for insider threats that includes different parts of an organization, such as human resources, personnel offices, physical security, and legal counsel. NIST 800-53 also offers control enhancements for insider threat programs. For example, the literacy training and awareness control can be supplemented by providing training on recognizing and reporting potential indicators of insider threats.
Committee on National Security Systems Directive 504 – Directive on Protecting National Security Systems (NSS) for Insider Threat	**Yes** The Committee on National Security Systems Directive 504 in Directive on Protecting National Security Systems (NSS) for Insider Threat requires that User Activity Monitoring (UAM) be implemented on all national security systems, both classified and unclassified, that contain information related to weapons systems and/or military operations.
Executive Order on Improving the Nation's Cybersecurity	**No** The EO on Improving the Nation's Cybersecurity (Cybersecurity EO) is a wide-reaching directive intended to improve federal government network security and increase security standards for private sector partners. The Cybersecurity EO includes guidance on sharing threat information, modernization, software supply chain security, incident and vulnerability response and detection, and investigation and remediation. While there are no specific comments on insider threat programs, the Cybersecurity EO does call for modernization of the federal government networks, including a requirement for a Zero Trust Architecture.
Executive Order 13800	**No** EO 13800 directs that each agency head use the Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology (NIST), or any successor document, to manage the agency's cybersecurity risk. The Framework was originally developed to assist Critical Infrastructure owners and operators with implementing a risk management approach to protecting their systems. Subsequently, the Framework has been widely adopted by companies and governments globally. It serves as an excellent guide for organizations of all sizes, in all sectors, for examining how they are managing their cybersecurity risk. While the Framework serves as a guide for approaching risk management, it does not provide any specific guidance with respect to insider threats.
Federal Information Security Management Act of 2002 (FISMA)	**No** The Federal Information Security Management Act of 2002 (FISMA) and its update, Federal Information Security Modernization Act in 2014, are some of the most prominent laws on protecting federal information and systems. Among other things, FISMA directs agencies to protect federal information and requires agencies to comply with federal standards, guidance, and policies related to federal information security. Additionally, FISMA provides broad authority to the director of the Office of Management and Budget (OMB) and the secretary of homeland security (DHS) to implement additional guidance around the protection of non-national security systems. FISMA also delegates similar authority for national security systems to the secretary of defense and the director of national intelligence.
Agency Personnel and Technology Policies	**Varies** Government agencies also have personnel policies and policies for behavior on government devices that describe allowed and prohibited behavior in the workplace. While these personnel and technical policies are important, inasmuch as they state the rules and let employees know what is and is not allowed, without any type of monitoring program, neither unintentional mistakes nor malicious behavior can be detected.

About Venable’s Cybersecurity Services Team

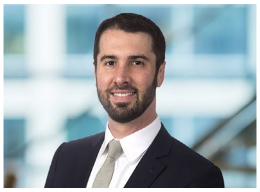
Fully immersed in all aspects of digital identity and cybersecurity, Venable stands apart among law firms and consulting firms because of its deep experience in standards, strategy, policy, and regulatory issues. Our team members draw on their past experiences working for and with various government and commercial entities in the privacy and technology landscape to provide solutions and insight into issues that impact our clients.

Our team has led policy development and implementation efforts at the White House National Security Council (NSC) and Office of Management and Budget (OMB), as well as in the Department of Defense, the National Institute of Standards and Technology (NIST), and the Department of Commerce. We participate in legislative advocacy, rulemakings, and development of new legal standards, and advise organizations with regard to industry best practices and drafting codes of conduct and standards, helping them stay compliant with federal, state, international, and self-regulatory requirements. We leverage our long-standing relationships with government officials and industry stakeholders to ensure that our clients have the best support and are the first to know about movement on existing and future policies, regulations, and legislation that affect their businesses. Our knowledge, experience, and relationships make us uniquely suited to provide in-depth reporting on topics and issues within the industry.

Author Biographies

Grant Schneider | Senior Director of Cybersecurity Services
Washington, DC | gmschneider@Venable.com | +1 202.344.4612

Grant Schneider is a recognized leader in the cybersecurity sector with extensive experience in driving organizational change, improving program maturity while reducing costs, developing policy and governance structures, and driving enterprise-wide technology modernization initiatives. Having served as the U.S. federal chief information security officer (CISO) based in the White House and on the White House National Security Council (NSC) as senior director for cybersecurity policy, Grant is uniquely positioned to assist clients in navigating the strategic, operational, and risk management needs of large-scale global technology environments.



Ross B. Nodurft | Senior Director of Cybersecurity Services
Washington, DC | rbnodurft@Venable.com | +1 202.344.4403

Ross Nodurft counsels clients on issues related to risk management, government policy standards and regulatory compliance, and incident management. Having served as principal of risk management and government solutions at a digital identity and cybersecurity firm and chief of the Office of Management and Budget's (OMB) Cyber Team in the White House overseeing federal government cybersecurity policy and federal agency incident response, Ross has significant experience with advising clients on how to navigate issues at the nexus of homeland security, technology, and cybersecurity policy.

Elizabeth Guillot | Cybersecurity Policy Analyst
Washington, DC | elguillot@Venable.com | +1 202.344.4574

Elizabeth Guillot assists clients with both domestic and international cybersecurity issues. Previously, Elizabeth was an associate manager of international policy at the U.S. Chamber of Commerce, where she focused on trade policy and digital economy issues to support the Chamber’s international trade advocacy. She has experience monitoring and analyzing high-priority policy issues, maintaining ongoing communication with government officials, and producing written products on behalf of companies across a variety of sectors. Elizabeth is currently pursuing an M.A. in security studies from Georgetown University.

VENABLE LLP