# COMBATING INSIDER THREATS

EXECUTIVE RESEARCH BRIEF

# INTRODUCTION

WikiLeaks. Edward Snowden. Bradley Manning. These highly publicized security breaches have recently brought insider threats into the eye of the mainstream.

However, federal government employees already know that insider threats are an ever-present hazard to government security and operations. In a recent GovLoop survey of over 153 public sector employees, 50 percent of respondents said their organization's level of concern over insider threats was high to very high, compared to only 23 percent who felt concern at their organization was low to very low.

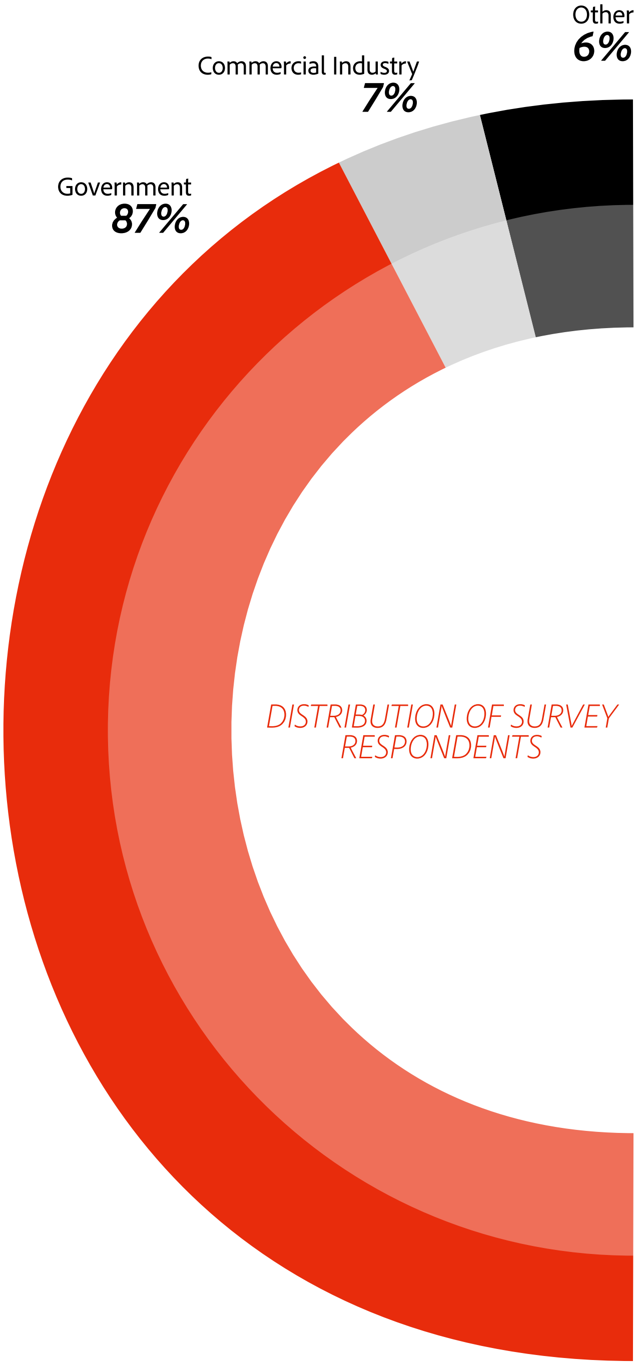
To learn how agencies can minimize the risk of insider threats without further burdening their overstretched agencies, GovLoop sat down with Patricia Larsen, Co-Director of the National Insider Threat Task Force (NITTF). We also investigated how deploying a secure content management system that monitors sensitive information across the lifecycle of a document can reduce insider threats.

There are limited security capabilities already in place within organizations. Amongst respondents who did know the protocols in place at their agency, digital signatures and encryption were the most common information management controls reported according to our survey.

However, only 27 percent of respondents said there was fine-grained access control within content management systems at their organization. Moreover, only 28 percent of respondents said their organization could discover in real-time when a document had been inappropriately accessed.

To keep their environments secure from insider threats, organizations must do more. This research brief:

- *Explains the risks associated with insider threats*
- *Identifies the barriers to implementing effective insider threat prevention programs*
- *Details the necessary components of a comprehensive content management system*



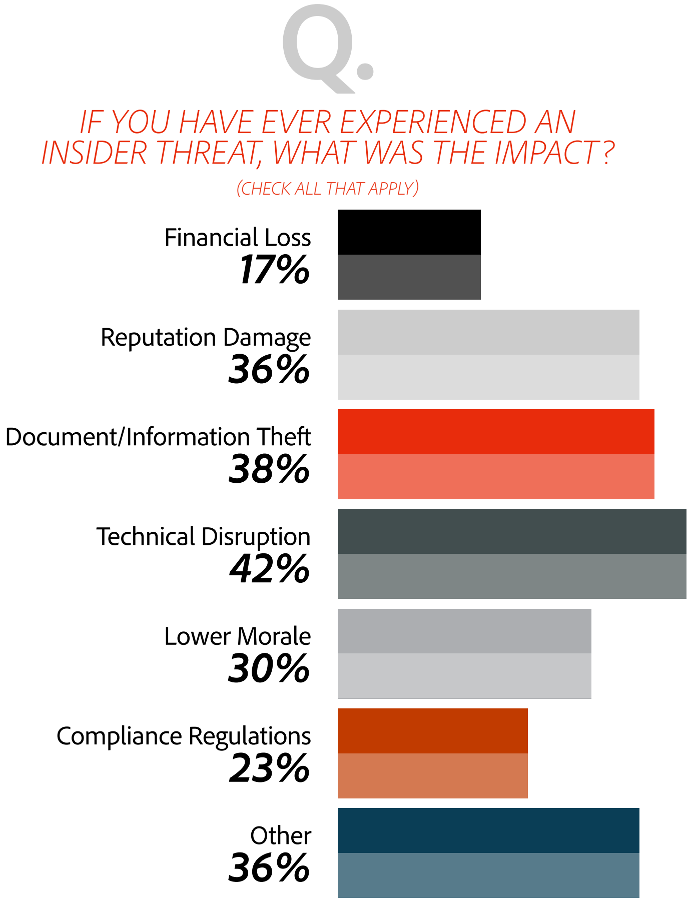
DISTRIBUTION OF SURVEY RESPONDENTS

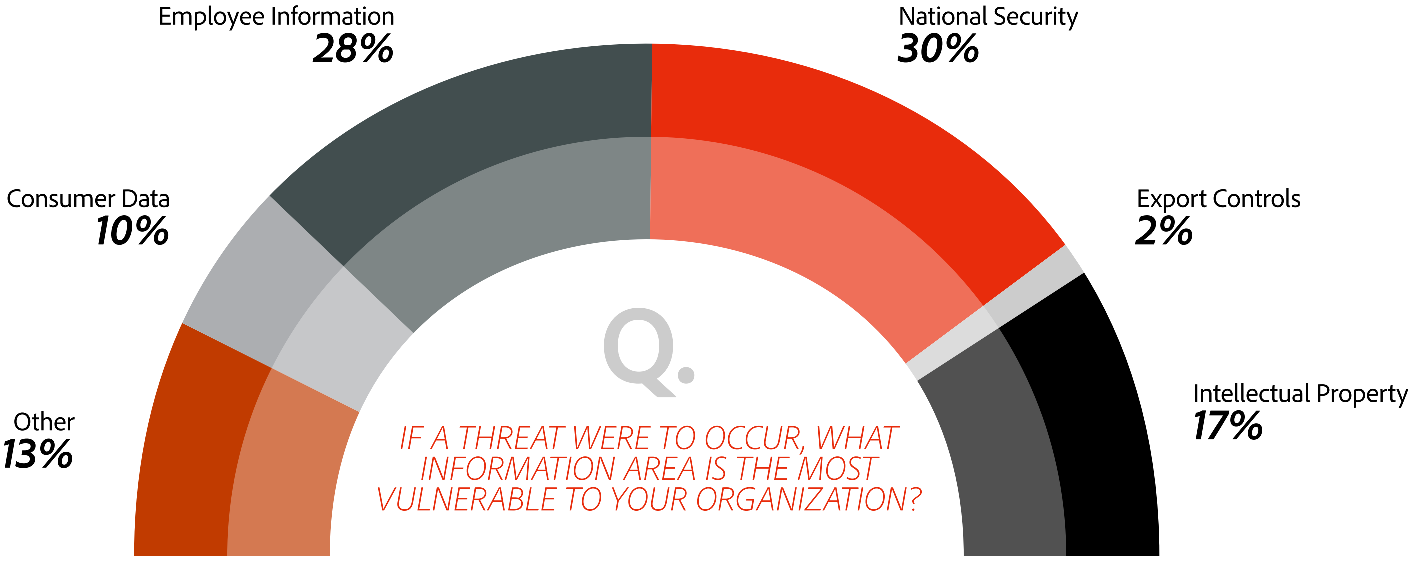
# THE RISKS OF INSIDER THREATS

The fallout from insider threats affects every facet of a government organization. Most obviously, when information is inappropriately distributed, national and agency security can be compromised. Of those respondents whose agencies had experienced an insider threat, 30 percent said that national security was the information area most vulnerable at their organization and 38 percent said previous threats resulted in document or information theft that compromised security.

Employees also feel the negative impact of insider threats. Their personal information may be exposed. Additionally, 42 percent of respondents said a previous leak led to technical disruptions in their workflow as processes were halted, investigated, or revised. Respondents also noted a loss of time, an increase in labor hours, and the need to retrain security staff as consequences of insider threats. As a result, 30 percent said that they witnessed lower morale among organization employees following a leak of information.

Finally, agencies also risk losing public support. 36 percent of survey respondents said their organization experienced reputation damage following an insider threat. This decreased public confidence can result in less funding from legislative bodies as well as diminished citizen engagement with agency services.





# CHALLENGES TO SECURITY

For most government organizations, recent high-profile events have only reiterated the need to manage information securely. Half of our survey respondents said that recent high-profile events have heightened concern at their agencies and made insider threats a higher agency priority. As a result, 45 percent of surveyed organizations implemented new security initiatives to reduce insider threats.

However, this last number could – and should – be higher. But according to our survey respondents, several obstacles prevent government agencies from effectively implementing better security initiatives. Budgetary constraints, cumbersome technology applications, and a lack of awareness among government employees challenge agencies' ability to form robust information management systems. We break down these challenges below.

## BUDGETARY CONSTRAINTS

Unsurprisingly, budget constraints are a major challenge to building insider threat management systems. Only 19 percent of respondents said the budget dedicated to preventing these threats was increasing in light of recent high-profile events. Therefore, it was predictable that 35 percent of respondents cited financial resources and 53 percent cited people resources as barriers to achieving an environment wholly protected from insider threats.

While concern for insider threats is high, many organizations lack the resources to execute new initiatives. As a result, security suffers.

## TECHNOLOGY

46 percent of respondents cited IT vulnerabilities as a barrier to achieving a secure information environment. This is often the result of budgetary constraints that limit the ability to acquire the most up-to-date systems. In other cases, technology is acquired but ineffectively incorporated into the existing IT security infrastructure.

To create an environment protected from insider threats, agencies must deploy information management systems that are easy to use and streamlined across the enterprise, despite budget limitations.

## AWARENESS

30 percent of survey respondents said confusion over governance of security policies and protections was a barrier to securing their information environment. In support of this perception, only 19 percent of respondents were aware of a leak of sensitive information from their organization within the last years. Moreover, an additional 28 percent of respondents admitted they were unsure if a leak had occurred. This suggests that communication around insider threats, and security-at-large, is lacking at most organizations.

Unfortunately, this lack of awareness about insider threat occurrences can significantly hinder security strategies. Without knowing the risks of insider threats, and how they happen at their organization, employees are more likely to underestimate the likelihood of threats and inadvertently put their information at risk of a leak.

Additionally, effective communication of insider threat mitigation efforts—even if specific tactics are not detailed—will build employee confidence in established processes and systems. As a result of knowing they are interacting with secure systems, employees are less likely to circumvent or misuse current security protocols to share sensitive information.

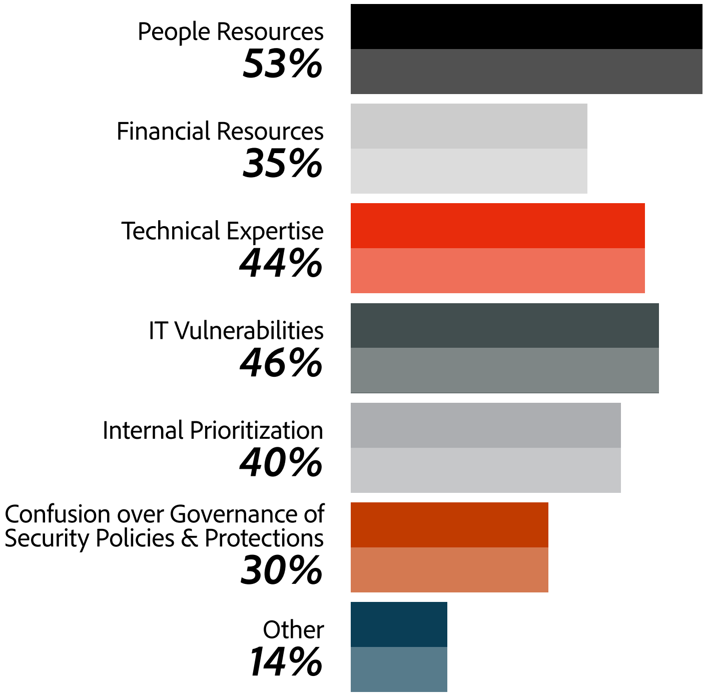
Yet many agencies have not appropriately communicated their insider threat counter tactics. More than half of our audience said that they were uninformed of their organization's information control strategies.

This lack of information challenges insider threat prevention because, even if strategies are in place, they are less likely to be executed uniformly or appropriately across the organization. Providing assurances to authors, recipients, and participants throughout electronic workflows is important because it gives them greater confidence. Without confidence in existing systems, personnel are likely to seek workarounds that, while believing they are adding safeguards, could actually decrease the security of information.

Q.

WHAT ARE YOUR ORGANIZATION'S BARRIERS TO ACHIEVING AN ENVIRONMENT WHOLLY PROTECTED FROM AN INSIDER THREAT?

(CHECK ALL THAT APPLY)



# COMPREHENSIVE CONTENT MANAGEMENT SYSTEMS AS A SOLUTION

Government organizations must holistically protect electronic information throughout their entire organization. Content management systems provide the means to do so, and counters many of the aforementioned challenges to creating a protected environment.

A comprehensive content management system can reduce the technology requirements of insider threat programs by streamlining processes while improving security. This single information management architecture also cuts costs by consolidating processes and technology contracts. And because this system is deployed throughout the entire IT environment, users become more aware of the technology in place to safeguard confidential information and the processes attached to them.

However, to reap these benefits organizations must deploy a total solution that is comprehensive, scalable, and applicable to multiple uses cases. Content management requires a number of interconnecting components, many of which are already deployed to some extent at government organizations. However, a piecemeal approach to securing information is likely to increase IT complexity and leave holes in your defenses.

In contrast, a comprehensive content management system safeguards against insider threats across three distinct domains: the repository of information, the content itself, and the users who access information.

## #1: PROTECT THE REPOSITORY OF INFORMATION

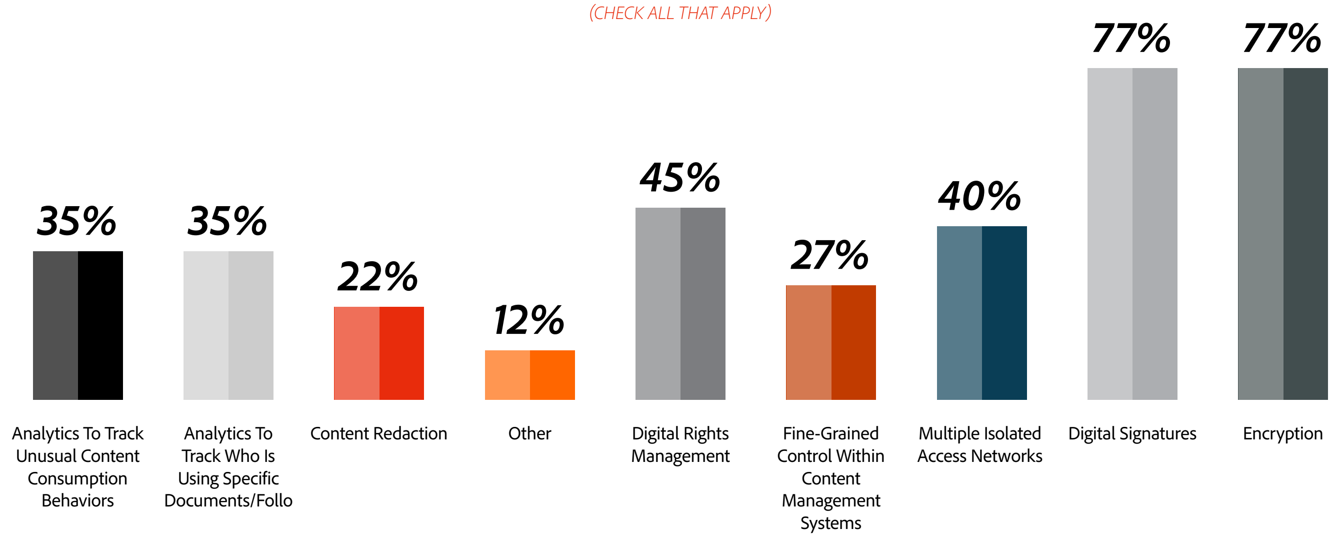
The first dimension of protection resides in information repositories where data is housed. Every time content is accessed, there is an authentication event to determine who is attempting to view it. Tactics such as digital rights management and digital signatures support this dimension by verifying the identity and permissions of users attempting to access files.

According to our survey, this is the content management dimension most often deployed by agencies. 77 percent of respondents use digital signatures while 45 percent use digital rights management as a means of authenticating file access. However, securing information from insider threats requires more robust protection measures that move beyond the repository of information.

Q.

WHICH CONTROLS DOES YOUR ORGANIZATION CURRENTLY EMPLOY TO COMBAT INSIDER THREATS?

(CHECK ALL THAT APPLY)



## #2: PROTECT THE CONTENT ITSELF

Protecting information beyond its initial location is the essential next step in mitigating insider threats. 72 percent of survey respondents said that employees or contractors at their agency must access information from mobile devices in order to execute their jobs. Yet only 23 percent of respondents were aware of controls in place at their agency to prohibit forwarding of a document once it is removed from content management systems.

Many organizations have invested in a portal or a content management system to control who has access to it. The challenge is that, once someone has access to that system, it's difficult to trace where that information is subsequently forwarded or how it is used. Securing the repository of information can only safeguard information while it is housed there.

Agencies must deploy tactics that continue to protect content from improper use, no matter where it goes. Therefore, rights management technology that persistently protects content at the content layer, independent of storage or transport, is a crucial component of any information security strategy.

For instance, a holistic solution will extend an access control list beyond a local repository.  That tactic forces encryption into the content itself, so that if a file is sent to someone lacking access privileges, they will be unable to access it. The only way to utilize the encryption key is to successfully log in to the agency system and have it determine that you are in the authorization list for that piece of content.

Unsurprisingly, 77 percent of respondent organizations use encryption methods. But while simple encryption safeguards against network or storage issues, it doesn't always prevent administrators from exploiting information. Increasingly, organizations are concerned about their administrators, because whoever has control of that content management system can see everything in it.

Separating encryption key management from content management is one way to tackle this challenge, because it ensures that no single person ever has access to all the documents and all the keys. A solution can be deployed where there is a separation of duties and systems between administering the content management system and administrating the rights management capability.

By encrypting documents and segmenting administration capabilities, the second dimension of content management protects documents beyond their file location on the agency server, and follows the content anywhere it goes.

## #3: MONITOR FOR UNUSUAL ACTIVITY

The third dimension of content management focuses on the way content is used. It's important to realize that insider threats are not always a case of employees accessing information above their access level. In many cases, insider threats are the result of employees mistakenly redistributing sensitive content. Therefore, in addition to protecting the file locations and documents themselves, an effective content management system will monitor for information being inconsistently or inappropriately accessed.

Only 35 percent of respondents said their organization deploys analytics to discover unusual content consumption behaviors. Yet inconsistent behavior can be a key indicator that an insider threat is taking place. This third dimension of associating audit logs of the content management and right management together can be very helpful for detecting unusual information access or unusually activity.

Monitoring unauthorized consumption patterns is a crucial component of insider threat prevention because it can alert administrators to threats before they are executed. Furthermore, when this dimension is effectively tied to information repository and document security, it creates added value for security teams and agency personnel.

From an administration perspective, a holistic content management system provides a streamlined infrastructure that provides a clearer picture of how information is used at the organization. At the same time, a cohesive system makes it easier for end users to access secure content with confidence.

# CREATING A ROBUST INSIDER THREAT PROGRAM AT ANY AGENCY

## AN INTERVIEW WITH PATRICIA LARSEN, CO-DIRECTOR OF THE NATIONAL INSIDER THREAT TASK FORCE (NITTF)

Insider threats are constant and varied within government, which can lead many agencies to think they are an inevitable occurrence. In reality, there are a number of tactics that agencies can pursue to mitigate the risk of an internal breach.

To better understand how government can minimize insider threats, we spoke with Patricia Larsen of the National Insider Threat Task Force. Larsen began our discussion by impressing the need for every agency that holds classified information to create an insider threat program.

## CUSTOMIZE YOUR STRATEGY

Larsen explained that most insider threat controls should be created and maintained by individual agencies. "Every different agency has a different mission, and they all know what's normal for their agency; what authorities their individual system administrators are supposed to have. So the analysis is best done closest to the point of where the mission is being accomplished."

This is especially important because indicators of potential threats must be customized to individual use cases. "There is no one single thing that you can point to and say that's an indicator of an insider threat," said Larsen. "You might see someone's doing an awful lot of printing late at night. That seems odd until you discover they work in a watch center so that's what their job is. You can't simply leap to a conclusion based on one indicator." However, this one indicator, coupled with previous incidents of questionable behaviors, could be valuable in determining if an individual is still clearance worthy.

Indicators of insider threats can be anything inconsistent with an individual's normal behavior. "It's identifying what's outside the norm for that individual or what kind of behavior that person is exhibiting that's different," said Larsen.

To identify those inconsistencies requires understanding individual roles and users. It also requires creating a mechanism to alert security to potential changes in behavior. Larsen said, "Agencies really need to have a system in place that will detect and flag if they see a massive exfiltration of information, for instance."

> “ **There is no one single thing** that you can point to and say that's an indicator of an insider threat.
>
> **– Patricia Larsen,**
> Co-Director of the National Insider Threat Task Force (NITTF)

## SCRUTINIZE USER PRIVILEGES

Larsen recommended three action steps to safeguard against insider threats. First, each user's privileges should be scrutinized. "We need to verify the access and privileges that each administrator has," she said. "Make sure they're commensurate with their job functions, their level of responsibility, and with their span of control that's required to do their job." Again, an agency-level understanding of user roles is crucial.

Among users, certain groups are more capable of committing large-scale insider threats. "Network administrators are a highly unique risk group," said Larsen. "They have access to a significant amount of information. They're often given the proverbial keys to the kingdom."

However, Larsen also said, "That's only if we let them… If we err on the side of convenience where we just grant more and more people network administrator access without thinking about who needs to do what, we're setting ourselves up for failure."

For this group, Larsen advises creating a second level of security to limit the privileges of any single administrator. Larsen suggested, "Enforce things like separation of duties so no one particular system administrator can do every possible function. And then you can require some sort of two-person control. So, if you have a sensitive location or network, you can require two people to be involved in protecting or servicing it." This ensures that any administrator access does not go unsupervised.

Finally, once privileges are diligently assigned to both administrators and less-privileged users they should be periodically reviewed on an individual and agency-wide basis to ensure they remain appropriate. Adjustments should be made as users are promoted, demoted, or exit the organization.

## COMMUNICATE YOUR STRATEGY

Once an agency has created a program to monitor potential insider threats, it's important to communicate the strategy to employees. Effective communication can both build buy-in for your program and strengthen your tactics' effectiveness.

Larsen explained that many agencies don't consider themselves part of the national security framework, and therefore don't think insider threats are a paramount concern at their organization. "One of the challenges that we've been facing is that we're asking for cultural change in some agencies that don't have a traditional national security mission. Their primary mission is something else to support the American population, and so they don't think about national security considerations first and foremost."

To combat this misconception, Larsen's team emphasizes how each agency serves a national security purpose and how their information could be compromised. "We give them examples of how adversaries have tried to target non-traditional information that their agencies hold. That gets their attention," said Larsen. When employees understand why protocols are important to security, they are more likely to follow them.

Additionally, agencies must communicate the tactics they will use to safeguard against insider threats. "You're not effective if you don't have a transparent program," said Larsen. "We have to set in general terms what is expected of employees."

Larsen also recommends encouraging employees to come forward if they see troubling or suspicious behavior. This mechanism provides an extra layer of security on the ground in your agency. It also creates an outlet for employees to seek help before they feel forced to commit unsafe actions. And while some employees may be reticent to vocalize concerns, Larsen said, "If you explain that you are here to help a person, not simply march them out the front door, then employees will be more supportive of the program. The goal is to protect the investment we have made in our people and our information."

This communication is admittedly a fine line. Larsen said, "Obviously you can't give a specific list of triggers and things that you're going to be looking for. You can't give away your playbook." This lesson returns to the need for customization. Depending on the scenario, agency mission, and individual user, the appropriate level of transparency will change.

Ultimately, agencies must determine how their mission fits within broader national security concerns. Larsen concluded, "Each agency has access to incredibly important information, and your agencies are critically important to our entire national security mission, not just to what you do as an individual department." Insider threat programs that are cognizant of that unique role are necessary to safeguard employees and their information.

# CONCLUSION

Following recent high-profile insider threats, agency leaders are under increased pressure to safeguard their organizations from employees who may accidentally or intentionally leak sensitive information. Yet barriers like technology complacency, budgetary constraints, and awareness prevent many agencies from securing their environment.

A robust content management system is one solution to these challenges. The streamlined security tactics provided by such systems span the lifecycle of documents to ensure that, no matter how information is accessed or utilized at your organization, it will be secure against malicious use. Implementation of a holistic system is a necessary step towards securing your agency against insider threats.

# ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 150,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to Hannah Moss, Research Analyst, at @hannahdmoss

GovLoop 1101 15th St NW, Suite 900 Washington, DC 20005

Phone: (202) 407-7421 Fax: (202) 407-7501

www.govloop.com

Twitter: @GovLoop

GOVLOOP
1101 15TH ST NW, SUITE 900
WASHINGTON, DC 20005
PHONE: (202) 407-7421 | FAX: (202) 407-7501
WWW.GOVLOOP.COM