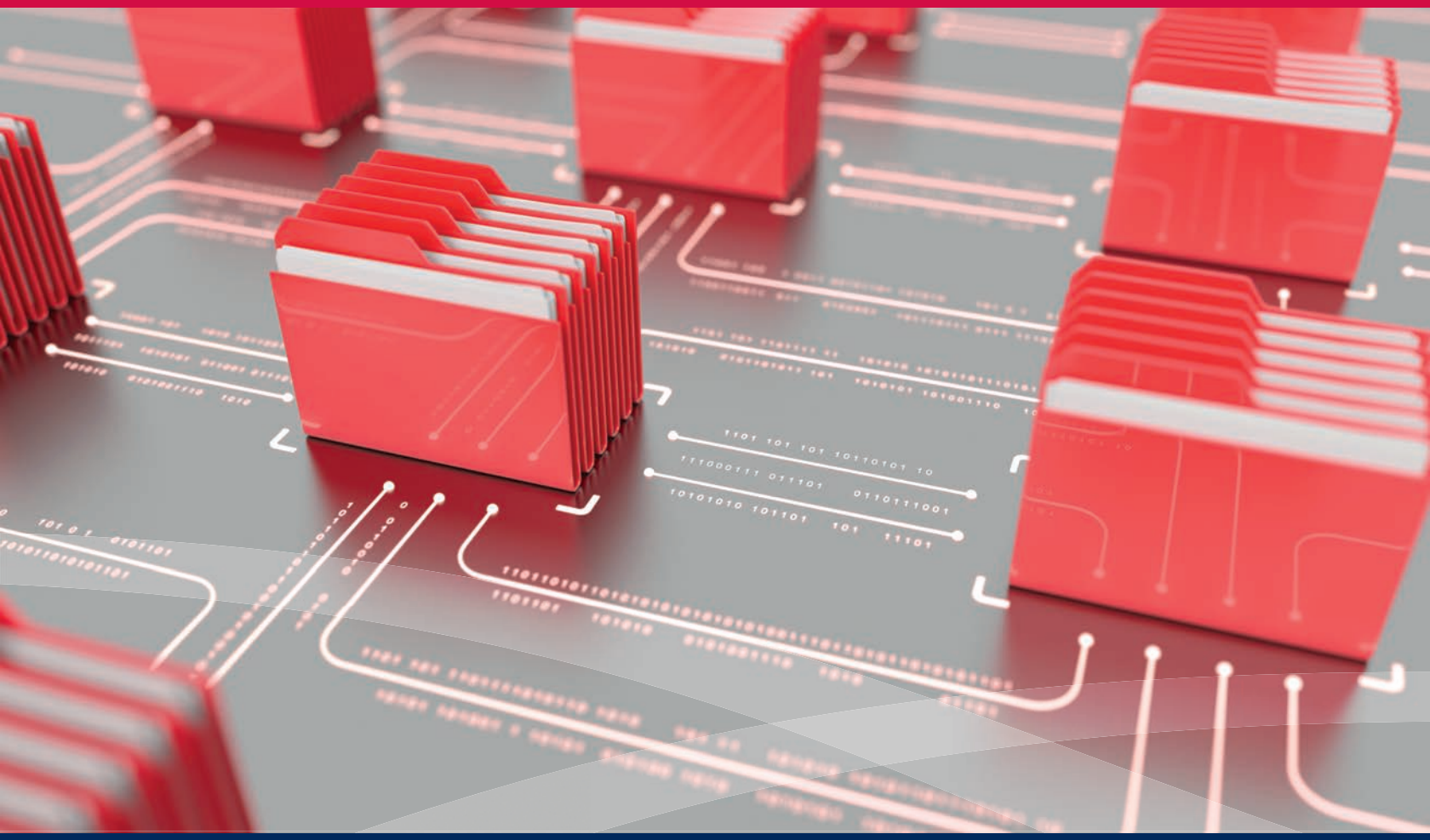


LEGAL HURDLES TO INSIDER THREAT INFORMATION SHARING

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Insider Threat Subcommittee

January 2020

INSA INSIDER THREAT SUBCOMMITTEE

INSA

ACKNOWLEDGEMENTS

INSA expresses its appreciation to the INSA members and staff who contributed their time, expertise, and resources to this paper.

INSA MEMBERS

Sandy MacIsaac, *Deloitte; Subcommittee Chair*

Vinny Corsi, *IBM; Subcommittee Vice Chair*

Julie Coonce, *TransUnion*

Kristin Grimes, *Leidos*

Joe Kraus, *ManTech*

Dave Luckey, *RAND*

Josh Massey, *MITRE*

Dan McGarvey, *Alion Science and Technology*

Donna Pucciarella, *AT&T*

Mike Seage

Tom Smith, *Department of Treasury*

INSA STAFF

Suzanne Wilson Heckenberg, *President*

Chuck Alsup, *Former President*

Larry Hanauer, *Vice President for Policy*

Peggy O'Connor, *Director, Communications and Policy*

Caroline Henry, *Marketing & Communications Assistant*

Megan Anderson, *Intern*

Jessica Willmore, *Intern*

INTRODUCTION

The large-scale theft and subsequent unauthorized release of classified information by Chelsea Manning and Edward Snowden, the arrest of Harold Martin and Reality Winner, and the Navy Yard shooting committed by Aaron Alexis all serve to highlight the risk posed by rogue members of the government's trusted workforce – those who have been fully vetted and granted access to the nation's most vital secrets, infrastructure, and workforce.

The postmortem into these and other acts of theft, espionage, sabotage, or workplace violence confirms that insiders often display similar characteristics or early warning signs. Agencies could and should do much more to identify anomalous behavior that indicates potential risk, assess potential threats, and respond accordingly.

The government has been taking steps to address such issues. For example, Executive Order (E.O.) 13587 – *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* – which established a National Insider Threat Task Force (NITTF), required that agencies implement insider threat detection and prevention programs with consistent minimum standards.[1] These initiatives were designed to strengthen national security through the improved sharing of "insider threat" information within and among agencies and defense contractors.

Many agencies and members of the national industrial base have taken aggressive steps to develop state-of-the-art threat detection programs that not only help protect classified and sensitive information but also identify the likelihood for workplace violence. However, two issues have become glaringly obvious.

- The first, based upon insights from industry, is the (perceived) inability of government agencies to share threat information with Cleared Defense Contractors (CDCs) even when the potential threat is an employee of the company. Government information is especially important, as most companies do not have the ability to monitor the activities of employees who use government networks at government facilities – often the first early warning sign.
- The second issue is the lack of threat information sharing among CDCs when employees leave one company to work for another.

The lack of transparency about the insiders who may pose threats means that these individuals can move freely between different jobs with contractors and government agencies, which results in transferring rather than solving the problem of insider threats.

Cleared industry organizations are significant targets of the United States' principal adversaries, who are seeking to modernize their militaries and strengthen their economies through the theft of U.S. intellectual property and of national security information that is outside of government hands. These nation-states frequently recruit or compromise insiders to further their aims. To protect both corporate and national secrets, the government's industry partners need basic personnel security information that can help identify and mitigate malicious insiders. Government information-sharing policies and the statutes that govern them should be reconsidered to permit greater information-sharing while still respecting employees' privacy and rights to due process.[2]

WHY SHARE INSIDER THREAT INFORMATION?

An insider threat is the threat presented by a person who has, or once had, authorized access to information, facilities, networks, people, or resources; and who wittingly, or unwittingly, commits: acts in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or destructive acts, to include physical harm to others in the workplace.

The most compelling reason to share information is that sharing substantiated derogatory information on staff and contractors is the only way to efficiently and comprehensively mitigate the threat of insiders who often change employers and/or clients. Cleared government contractors often rotate among agencies, which prevents any one organization from developing a comprehensive portrait of an employee's work habits, personal and professional stressors, and core beliefs. Cleared contractors may support multiple agencies at the same time, and they may change firms; both dynamics cause a fragmented view of employees' behavior. When government agencies fail to share derogatory information on individuals' behavior to contractors' employers, the result is that no single repository for such information on an individual exists, making it difficult for any entity to take action to mitigate risks.

One of the most glaring examples of this need to share information is the Washington Navy Yard shooting perpetrated by Aaron Alexis. On September 16, 2013, Alexis, a civilian contractor supporting the Navy and a vetted member of the U.S. Navy Individual Ready Reserve with a Secret security clearance, used a valid badge to enter the Washington Navy Yard, where he killed 12 people and injured four others. The Department of Defense "Internal Review of the Washington Navy Yard Shooting"[3] concluded that "At various points during Alexis's military service and subsequent employment as a cleared contractor – from the background investigation in 2007 to the disturbing behaviors he exhibited in the weeks leading up to the shooting – the review revealed missed opportunities for intervention that, had they been pursued, may have prevented the tragic result at the Washington Navy Yard." The report emphasized that a review of individual data points yielded little insight; combined, however, these disparate data points demonstrated a pattern of misconduct and disturbing behavior.

LEGAL PRECEDENT SUGGESTS AN OBLIGATION TO SHARE

By not sharing factual, substantiated derogatory information, employers may incur liability on a number of fronts to include under tort law and certain statutes.

Typically, an employer will not be liable for the actions of its employee under the rule of *respondeant superior* if the acts are outside the scope of employment and not intended to further the employer's benefit. However, liability may still attach if an employer is willfully blind[4] to activity (i.e., if it suspects wrongdoing and fails to investigate).

> To protect both corporate and national secrets, the government's industry partners need basic personnel security information that can help identify and mitigate malicious insiders.

Under a tort theory of negligence, if an employer has knowledge of an employee's behavior that may affect the safety of others but fails to take action, the employer may be at risk of a negligent retention or supervision claim by a coworker or other third party injured by the employee.[5] As in all negligence claims, the injured party must prove certain elements, and though these vary by state, these generally include: a relationship between the employee and employer existed; the employer knew or should have known of the threat or incompetence; the employee's conduct caused the injury or reasonable apprehension of such; the employer retained or failed to supervise the employee; and actual damage resulted.[6] Under a similar theory, failing to notify a new employer about a departing problem employee could impose liability on the former employer if the problem employee repeats the misdeed at the new company.

There is a common law duty to report issues in order for an employer to exercise reasonable care to prevent harm to others.[7] Even if an employee is acting outside the scope of employment, the employer may have this duty. In some courts, there is no liability in tort for former employers for failure to warn of or control an employee's future conduct by reporting to authorities.[8] Despite the absence of common law duties, there may be statutory duties to report.

Laws and regulations that require employers to share information include the Occupational Safety and Health Act (OSHA), which imposes on employers a general duty to provide a safe working environment. OSHA suggests reporting threatened or actual violent incidents to the police. Under Change 2 to the National Industrial Security Program Operating Manual (NISPOM), which provides security guidance to cleared contractors, firms are required to "gather, integrate, and report relevant and available information indicative of a *potential* or actual insider threat…"[9] (Emphasis added.) However, it is often difficult to obtain the level of detail needed to determine whether a threat exists from reports in government databases that track clearance accesses and security violations, such as the Joint Personnel Adjudication System (JPAS).

CASE STUDY: AARON ALEXIS AND THE NAVY YARD SHOOTING

In the wake of the Washington Navy Yard shooting, victims and family members brought suit against Alexis's employers for a variety of claims. In the case of *Jennifer Jacobs v. The Experts, Inc.,*[10] Plaintiffs assert a combination of negligence and intentional tort claims against HP Enterprise Services, LLC (HPES) (now known as Enterprise Services, LLC), which provided information technology services to the U.S. Navy as a government contractor, and The Experts, Inc. (The Experts), which was an HPES subcontractor and Mr. Alexis' employer.

Under D.C. law, third party liability is subject to different tests depending on the nature of the allegation. On one hand, a negligence claim for failure to prevent a criminal act, which does not rely on a duty to control or supervise, has a higher standard requiring specific evidence of foreseeability.[11] There is a lower standard for foreseeability when it comes to negligent retention and supervision, which requires a plaintiff to "show that an employer knew or should have known its employee behaved in a dangerous or otherwise incompetent manner, and that the employer, armed with that actual or constructive knowledge, failed to adequately supervise the employee."[12]

In this case, on September 15, 2016, the U.S. District Court judge ruled in favor of HPES and The Experts that the facts were insufficient to plead Alexis' criminal conduct was foreseeable. However, the judge ruled that Plaintiffs' claims of negligent retention and supervision could continue against Alexis' former employers. Follow-on litigation with different plaintiffs alleging similar actions against the defendants resulted in consistent rulings by the court, dismissing all counts against all defendants other than those alleging negligent retention and supervision. The cases have settled rather than going to judgment before the court, but similar cases and a 30-year history in the D.C. Court of Appeals have reinforced the lower standard of foreseeability to prove an employer's negligent retention and supervision.

LEGAL HURDLES TO INFORMATION SHARING

Despite reasons to share that in some cases are legally mandated, organizations hesitate before doing so. Concerns over protections afforded to individuals have deterred elements of information sharing that are arguably permissible. The fear of litigation or censure has caused legal departments to take the risk averse approach of staying far away from the line. A better understanding of where that line is should help to inform such legal decisions, and ideally will permit increased information sharing resulting in more robust insider threat mitigation programs.

Generally, companies are on safe ground as long as they report to the government documented information regarding an employee's performance that has a clear link – under the law or regulatory materials such as the NISPOM – to the employee's ability to secure or maintain a security clearance. Such reporting and any related adverse actions should be applied consistently across the workforce and should not, through inappropriate coordination, generate an anti-competitive effect. Laws that impact such information sharing are summarized below.[13]

The risk exists that *inaccurate* derogatory information could unfairly tar an employee as a security risk; if such information is shared with an employer, the employee could suffer adverse action, including the loss of employment and the loss of security clearance eligibility. While delaying remedial action could exacerbate any security risk that exists, agencies should make reasonable attempts to confirm or validate their concerns before sharing derogatory information about an employee with his/her employer.

DISCRIMINATION

Decisions to share adverse information could result in discrimination, retaliation, or harassment claims. While employers may legally share the reasons for an employee's termination, they should do so carefully. To start, employers should internally document the reasons for termination to prove the existence of legitimate grounds for an adverse employment action as opposed to a pretext for improper action. Similarly, an employer should be consistent when taking adverse actions against employees and in choosing what types of information to communicate to prospective employers to avoid claims of disparate treatment.[14] This is particularly true when considering employees of a protected class.

WRONGFUL TERMINATION

Sharing adverse information in the form of reporting to the government may result in an individual's loss of his or her security clearance. In some cases, loss of a clearance can also result in loss of employment if the clearance is required for the position. This presents a particular problem if the reported activity is later found to be incorrect.[15] Employers should keep these considerations in mind as they balance NISPOM reporting requirements and decisions to share information. Focusing on the details of employee behavior or comments – particularly those that have been investigated, substantiated, and found to be credible – without subjective color to reporting, is the best way to strike this balance.

DEFAMATION

Companies are often reluctant to share information about employee misconduct because of a fear that the employee will claim the company defamed him/her. However, an employer's qualified privilege protects it when sharing certain performance-related information, and Supreme Court precedent supports contractors' responsibility to report to the government information regarding cleared employees that indicates potential security risks.

Defamation laws vary by state, but certain concepts generally apply. Defamation is a written (libel) or oral (slander) statement that damages the reputation, character, or good name of another person. False statements that disparage another in the conduct of his business are considered defamation per se, meaning that the one making the defamatory statement is subject to liability even if no special harm results.[16] Defamatory statements in this category include those accusing the individual of fraud, misconduct, dishonesty, incapacity, or lack of qualifications.[17] If defamatory statements are communicated to the public at large, the publisher may also face allegations of the tort of false light.

A statement must be false in order for it to be defamatory.[18] While this may provide some latitude to an employer to share information about an employee that is negative, the employer must take care to state facts. Misinterpretation or misrepresentation of facts, or a mistaken belief in the truth of the matter, are not sufficient to leverage this defense.

Expressions of opinion cannot give rise to a defamation claim. However, an employer must be careful not to co-mingle opinions and facts. If any part of a statement contains a factual allegation, the entire statement, including the opinion, could be the basis for a defamation claim.[19]

There remains the threat of "self-publication", wherein the employer makes a defamatory statement to an employee as part of its grounds for termination, and the employee repeats the statements to a potential employer.[20] Some courts allow recovery if the employer knew or could have foreseen that the employee would repeat or be compelled to repeat the defamatory statement. These types of claims may be defeated by an employer's qualified privilege to make the statement.

> ...case history makes clear that contractors may report to the government information regarding cleared employees that indicates potential security risks.

Qualified privilege allows for negative performance evaluations, statements to prospective employers, and disclosures to customers and coworkers regarding an employee's termination.[21] The communication must be done in good faith, and when to a prospective employer, must be issued at the request of that party or the former employee, and the prospective employer must have an important interest in the information.[22] Several states have statutes that protect employers when providing job references. For example, in Virginia, upon request by a prospective or current employer, employers can provide information about a person's professional conduct, reasons for separation, or job performance, including, but not limited to, information contained in any written performance evaluations. Immunity from civil liability only attaches if the employer is not acting in bad faith, and is presumed to be acting in good faith.[23]

There are also bases for absolute and qualified privilege for communications made to police, though this depends on jurisdiction and situation-specific facts. Another defense that varies by state is if the statement is based solely on an opinion on a matter of legitimate public interest even though it may negatively affect someone's reputation.[24]

As the NISPOM notes, in *Taglia vs. Philco,*[25] the U.S. Court of Appeals for the 4th Circuit decided that a contractor is not liable for defamation of an employee because of reports made to the Government under NISPOM requirements. In *Becker v. Philco* (389 U.S. 979), the U.S. Supreme Court denied the appeal from the 4th Circuit. This case history makes clear that contractors may report to the government information regarding cleared employees that indicates potential security risks.

ANTITRUST

In October 2016, the U.S. Department of Justice and the Federal Trade Commission released guidance that companies and individuals would be subject to both criminal and civil prosecution for violating antitrust laws.[26] This includes employers and the prohibition against creating unlawful agreements not to compete. Different types of information sharing with competitors can result in antitrust law violations, to include data about wages, benefits, and employment terms.[27]

No-poaching agreements, whereby one company agrees that it will not solicit or hire the other company's employees, and naked wage fixing, are per se illegal.[28] As the guidance notes, even without explicit coordination to fix compensation or other employment terms, "exchanging competitively sensitive information could serve as evidence of an implicit illegal agreement."[29] However, agreements to share information are not per se illegal but may be subject to civil antitrust liability when they have, or are likely to have, an anticompetitive effect.[30]

Coordination between companies concerning an employee's questionable behavior or insider threat case could bring claims of unlawful agreements not to compete. In some instances, having a neutral third party manage such information can mitigate antitrust concerns,[31] such as using the below-described DoD Insider Threat Management Analysis Center (DITMAC) system or a similar Information Sharing and Analysis Organizations (ISAO)/Information Sharing and Analysis Centers (ISAC). The Department of Justice (DOJ) Antitrust Division has a business review process[32] to determine how the Division may respond to proposed business conduct, and the Federal Trade Commission (FTC) offers similar advisory opinions.[33]

DUE DILIGENCE IN SCREENING AND REPORTING

More detailed insight into initial hiring and background checks are beyond the scope of this paper; however, appropriately designed investigations and due diligence at this stage are essential, particularly for sensitive positions. For example, employers should use caution when considering consumer reporting agency data to ensure the data meets notification and time restrictions. Further, employers should be mindful of the abundant federal and state laws concerning arrest and conviction records.[34]

Certain laws and regulatory bodies recognize that some jobs are more sensitive and therefore permit more aggressive screening and reporting. This is particularly true for positions requiring security clearances. Title VII of the Civil Rights Act of 1964, for example, allows employers to decline hiring an individual if s/he cannot satisfy statute- or Executive Order-imposed security clearance requirements or is unlikely to timely obtain a required clearance.[35] This is an affirmative defense to a discrimination charge, so employers must assert that defense and both demonstrate the legitimate national security requirement and provide evidence that the individual in question has not fulfilled or has ceased to fulfill that requirement.[36] Employers should take care to apply the law consistently and never selectively to members of a protected class or to positions not subject to national security requirements.

For helpful guidance on the legal challenges in this area, see the ACC Docket's 2017 publication, *How Employers Can Mitigate Insider Threats.*[37]

RECOMMENDATIONS

Cleared industry and the government can help each other meet the shared goal of strengthening insider threat programs without running afoul of the legal pitfalls discussed above. Potential solutions include information sharing mechanisms, new legislation, and better use of existing government-created groups.

DEVELOP A UNIFORM INTERPRETATION OF THE PRIVACY ACT

Government lawyers should agree upon a uniform, government-wide interpretation of what information can be shared with industry under the Privacy Act. Certain disclosures by the government are already permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended. Under this, records may be disclosed outside of DoD as a routine use pursuant to 5 U.S.C. 552(b)(3). Subject to change with future revisions, current routine uses of this system include decisions:

> "concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, delegation or designation of authority, or other benefit, or if the information is relevant and necessary to a DoD decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, delegation or designation of authority, or other benefit and disclosure is appropriate to the proper performance of the official duties of the person making the request."

To extend this to the private sector might require a revision to the terminology used in the Privacy Act, particularly "agency;" however, any government contractor, especially DoD contractor, is arguably an agent of the government and may be covered.

Further, routine uses of this DoD system include sharing a:

> "record consisting of, or relating to, terrorism information, homeland security information, counterintelligence, or law enforcement information may be disclosed to a Federal, state, local, tribal, territorial, foreign government, multinational agency, and to a *private sector agent* either in response to its request or upon the initiative of the DoD Component, for purposes of sharing such information as is necessary and relevant to the agency's investigations and inquiries related to the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America as contemplated by the Intelligence Reform and Terrorism Protection Act of 2004." [emphasis added]

To ensure consistency across government, the Office of Management and Budget (OMB) and the Office of the Director of National Intelligence (ODNI) should convene an interagency legal working group to develop a common interpretation of what derogatory data on individual contractors can be shared under the Privacy Act with the individuals' employers. If statutory changes are needed to share information that could mitigate security threats, OMB should propose such changes to Congress.

EXPAND DITMAC AND DOD COMPONENT INSIDER THREAT RECORDS SYSTEM TO THE PRIVATE SECTOR

As noted above, DOJ and FTC have stated that using a neutral third party to manage information sharing can mitigate antitrust concerns.[38] Leveraging ISAOs/ISACs[39] could provide requisite third-party management of information to insulate against antitrust claims.

Another option is to expand the existing DoD Insider Threat Management and Analysis Center (DITMAC) and DoD Component Insider Threat Records System to the private sector. The system is used to analyze, monitor, and audit insider threat information for insider threat detection and mitigation within DoD on threats that insiders may pose to DoD and U.S. Government installations, facilities, personnel, missions, or resources. Currently each of the 44 DoD Insider Threat Component Hubs has its own instance of the system in order to keep component information segregated. If information meets a certain threshold, it is referred to DITMAC, which may then also see the data.

Expanding this system to CDCs would require a fundamental shift in the existing scope of DITMAC sharing, as well as establishment of criteria for sharing that is acceptable to CDC lawyers and approved by all 44 DoD Components. These requirements present significant hurdles, but the concept is worthy of consideration given the more comprehensive picture of the workforce that it could create. It would assist the private sector to learn of insider threat-related details when making a hiring decision or a decision to sponsor an individual's clearance. This will also support the government's insider threat mitigation goals and will increase security through the additional parties evaluating and culling individuals with access to classified and sensitive information.

Further, the DoD Component Insider Threat Records System is intended to facilitate the identification of best practices within the government. Best practices developed by the private sector would be similarly informative to the government, and thus this expansion to the private sector would benefit all parties.

MODIFY SF-86 CONSENT AND DISCLOSURE LANGUAGE

Another option would be to obtain consent from security clearance applicants in their SF-86, the form used to submit biographical data necessary for a clearance investigation. For example, adding language such as, "By virtue of submitting for a clearance, you consent that the Central Adjudication Facility can and will share any information pertaining to the scope of this document and adjudicative decisions with your employer, to include government agencies or commercial businesses that have an employer-like role." This would require a revision to the form through a normal draft and review process. The promulgation of new forms across the cleared workforce would take more than a decade to fully implement, as employees with Secret-level clearances must submit forms for reinvestigation every ten years.

PASS LEGISLATION TO CREATE INSIDER THREAT INFORMATION SHARING PROTECTIONS MODELED ON CISA

In the cyber world, industry faced similar challenges. As McAfee Labs Threats Report noted, in 2015 more than 50 percent of organizations believed that company policy would prevent cyber threat information sharing, while about 25 percent believed industry regulations would prevent it.[40] The U.S. Government recognized this issue and the need for information sharing and created a legal regime to facilitate such activity. The U.S. Cybersecurity Act of 2015 provides a legal foundation for sharing between the government and private sector, as well as within the private sector. The Act further provides liability protection if sharing is done as outlined by the legislation.

Title I of the Cybersecurity Act, the Cybersecurity Information Sharing Act of 2015 (CISA), provides protections for companies to share "cyber threat indicators" and "defensive measures" with covered entities. Cyber threat indicators include malicious reconnaissance, methods for defeating security controls, security vulnerabilities, methods of causing a user with legitimate access to unwittingly enable the defeat of a security control or exploitation of a security vulnerability, malicious command and control, and actual or potential harm caused by an incident.[41]

CISA provides protection from liability for cyber information sharing when done in accordance with the requirements defined in the law.[42] It also exempts sharing from federal and state antitrust violations when done to prevent, investigate, or mitigate threats.[43] CISA requires that certain information be removed before sharing, to include Protected Health Information (PHI), Human Resources Information, Consumer Information/History, Financial Information, and phishing targets' names and email addresses.

Insider threat indicators are similar to cyber threat indicators. Insider threat indicators provide insight into the actual harm caused by an employee's behavior, giving insight into the potential harm that similar behavior could cause to another organization. Insider threat indicators under the same model would include witting and unwitting insiders using technical and non-technical means to conduct physical and cyber reconnaissance, defeat security controls, create and exploit vulnerabilities, and exert control over systems, information, and facilities.

Granting similar legislative protections from liability and antitrust violations would be a much-needed tool to facilitate sharing of insider threat indicators. However, gathering the political will to pass a similar bill in Congress would be more of a challenge due to the privacy concerns. The information that would need to be included in such sharing inherently would be the type of information that is required for removal under CISA and that likely made passage of the bill more palatable. The indemnity provision for insider threat information sharing should require adhering to strict standards of limiting and protecting such information, as well as freedom from liability unless gross negligence.

LEVERAGE THE NATIONAL INSIDER THREAT TASK FORCE

In another corollary to the cyber world, having a task force of powerful stakeholders is a critical element to realizing necessary change. In 2008, the Office of the Director of National Intelligence (ODNI) established a Joint Interagency Cyber Task Force to coordinate cyber activities and cross-agency participation. This produced laudable results and set the stage for leveraging the task force model to tackle similarly difficult issues. In October 2011, E.O. 13587 established the National Insider Threat Task Force (NITTF) to assist federal departments and agencies with the creation and implementation of insider threat detection and prevention programs.

It is critical that the government use NITTF to its fullest potential, including maximizing coordination with the private sector. NITTF frequently publishes helpful resources for the insider threat community to use in executing and improving programs. The NITTF should create a resource on information sharing guidance that addresses the challenges outlined in this paper would significantly assist both government and private industry entities.

One example of this already coming to fruition is the NITTF Insider Threat Program Maturity Framework[44] which highlights as one element (ME17) of program maturity the necessity for documented "procedures and agreements with other USG (U.S. government) InTPs (Insider Threat Programs) to request or refer information on insider threats of mutual concern."

CREATE A SEARCHABLE REPOSITORY OF DEROGATORY BEHAVIOR THAT INDUSTRY CAN ACCESS

The relative sparseness of statutory reporting requirements calls for criminalization of certain behaviors so that contractors have a duty to report. The requirement to report should result in searchable memorialization of reportable behavior in background records. It would also help to address a problem the U.S. Supreme Court has identified, that the "gross indifference to the duty to report known criminal behavior remains a badge of irresponsible citizenship".[45] Responsible citizens, however, need protections as detailed above.

CONCLUSION

While there are challenges to the problem of insider threat information sharing, the severe national security consequences of not sharing data on concerning behavior by cleared employees should drive efforts to overcome those challenges. Sharing basic personnel security information with contractors' employers – particularly substantiated reports of inappropriate conduct – would enable cleared contractors to investigate employees of concern, make full use of their government-mandated insider threat programs, and take appropriate action to reduce security risks. The federal government must consider modifications to existing legal frameworks, new legislation, and robust collaboration with industry partners to mitigate insider threats effectively.

REFERENCES

[1] *White House, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, Executive Order 13587, October 7, 2011. At https://obamawhitehouse.archives.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net.*

[2] *A number of potentially relevant legal issues are beyond the scope of this paper; they include negligent hiring, intentional infliction of emotional distress, trade libel, tortious interference with contact, and malicious prosecution.*

[3] *U.S. Department of Defense, Internal Review of the Washington Navy Yard Shooting, November 20, 2013. Available at https://archive.defense.gov/pubs/DoD-Internal-Review-of-the-WNY-shooting-20-Nov-2013.pdf.*

[4] *See United States v. Bank of New England, N.A., 821 F.2d 844, 856 (1st Cir. 1987))*

[5] *Reporting Criminal Activity of Employees, Practical Law Practice Note w-008-1471 (2018), p16.*

[6] *Reporting Criminal Activity of Employees, Practical Law Practice Note w-008-1471 (2018), p16.*

[7] *§ 317 Duty of Master to Control Conduct of Servant, Restatement (Second) of Torts § 317 (1965).*

[8] *San Benito Bank & Trust Co. v. Landair Travels, 31 S.W.3d 312, 318, 321-22 (Tex. App.—Corpus Christi 2000, no pet.)*

[9] *U.S. Department of Defense, National Industrial Security Program Operating Manual, Incorporating Change 2, May 18, 2016. Available at http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522022M.pdf*

[10] *Jennifer Jacobs v. The Experts, Inc., 212 F. Supp. 3d 55 (D.D.C. 2016)*

[11] *See Boykin v. District of Columbia, 484 A.2d 560 at 564–65 (D.C.1984); Lacy v. District of Columbia 424 A.2d 317 at 323–24 (D.C.1980) (Lacy II). "Where an injury is caused by the intervening criminal act of a third party, [District of Columbia Court of Appeals] has repeatedly held that liability depends upon a more heightened showing of foreseeability than would be required if the act was merely negligent." Bailey v. District of Columbia, 668 A.2d 817, 819 (D.C. 1995).*

[12] *Giles v. Shell Oil Corp., 487 A.2d 610, 613 (D.C. 1985).*

[13] *Nothing in this paper is intended to be legal advice. Each company needs to perform its own risk assessment as it considers program implementation.*

[14] *Reporting Criminal Activity of Employees, Practical Law Practice Note w-008-1471 (2018), p15.*

[15] *Schwartz, Daniel, et al., New insider threat regulations to hit contractors hard, Bloomberg Government (Nov 2016) https://about.bgov.com/blog/new-insider-threat-regulations-hit-contractors-hard-2/*

[16] *§ 570 Liability Without Proof of Special Harm—Slander, Restatement (Second) of Torts § 570 (1977). Special harm or damages are economic or financial losses that result from the reputational injury.*

[17] *Defamation Basics, Practical Law Practice Note w-001-0437 (2017)*

[18] *§ 581A True Statements, Restatement (Second) of Torts § 581A (1977)*

[19] *Defamation Basics, Practical Law Practice Note w-001-0437 (2017) p7.*

[20] *Defamation Basics, Practical Law Practice Note w-001-0437 (2017); Wright v. Keokuk Cty. Health Ctr., 399 F. Supp. 2d 938, 957-58 (S.D. Iowa 2005)).*

[21] *Defamation Basics, Practical Law Practice Note w-001-0437 (2017) p8.*

[22] *Defamation Basics, Practical Law Practice Note w-001-0437 (2017) p8; (Erickson v. Marsh & McLennan, 569 A.2d 793, 805-06 (Sup. Ct. N.J. 1990).)*

[23] *VA Code Ann. § 8.01-46.1, Disclosure of employment-related information; presumptions; causes of action; definitions.*

[24] *Defamation Basics, Practical Law Practice Note w-001-0437 (2017) p7; See Magnusson v. N.Y. Times Co. d/b/a KFOR, 98 P.3d 1070, 1075 (Okla. 2004).)*

[25] *Taglia vs. Philco, 372 F.2d 771 (4th Cir. 1967).*

[26] *Department of Justice, Federal Trade Commission, Antitrust Guidance for Human Resource Professional (October 2016); available at https://www.justice.gov/atr/file/903511/download.*

[27] *Noack, Sarah. Federal Antitrust Guidance for HR Professionals, Indiana Employment Law Letter, 26 No. 12 Ind. Emp. L. Letter 4, (Dec. 2016). Westlaw.*

[28] *That is, they are deemed illegal without any inquiry into its competitive effects. See DOJ/FTC Antitrust Guidance for HR Professionals at p. 3.*

[29] *DOJ/FTC Antitrust Guidance for HR Professionals at p. 4.*

[30] *DOJ/FTC Antitrust Guidance for HR Professionals at p. 4.*

[31] *DOJ/FTC Antitrust Guidance for HR Professionals at p. 5. However, DOJ/FTC suggests the factors for permitting information sharing are conjunctive, also requiring that the exchange involves information that is relatively old, the information is aggregated to protect the identity of the underlying sources, and enough sources are aggregated to prevent competitors from linking particular data to an individual source.*

[32] *DOJ, Introduction to Antitrust Division Business Reviews, https://www.justice.gov/sites/default/files/atr/legacy/2011/11/03/276833.pdf.*

[33] *FTC, Competition Advisory Opinions, https://www.ftc.gov/tips-advice/competition-guidance/competition-advisory-opinions.*

[34] *Erika Schenk, Brian Kaveney, and Brad Bakker, How Employers Can Mitigate Insider Threats, 35 No. 3 ACC Docket 32 (April 2017).*

[35] *See EEOC, Policy Guidance on the use of the national security exception contained in § 703(g) of Title VII of the Civil Rights Act of 1964, as amended, No. N-915-041 (May 1, 1989); Title VII of the Civil Rights Act of 1964, as Amended, §703(g).*

[36] *See In Molerio v. F.B.I., 749 F.2d 815 (D.C. Cir. 1984) (upholding FBI's refusal to hire Molerio as a special agent after he failed to obtain security clearance due to his ties to Cuba).*

[37] *Erika Schenk, Brian Kaveney, and Brad Bakker, How Employers Can Mitigate Insider Threats, 35 No. 3 ACC Docket 32 (April 2017).*

[38] *DOJ/FTC Antitrust Guidance for HR Professionals at p. 5.*

[39] *Presidential Executive Order 13691 directed the DHS to fund a nongovernmental organization to serve as the ISAO Standards Organization. The ISAO Standards Organization was created to identify a set of voluntary standards and guidelines for the creation, operation, and functioning of cyber sharing and analysis organizations. The intent is to expand the current sector-based model (financial, health, energy, etc.) of Information Sharing and Analysis Centers, enabling the development of innovative types of threat information sharing organizations using standard interoperable interfaces and data formats. McAfee Labs Threats Report, March 2016, p15.*

[40] *McAfee Labs Threats Report, March 2016, p11.*

[41] *Cybersecurity Act of 2015 (CISA), Sec. 102(6)*

[42] *Cybersecurity Act of 2015 (CISA), Section 106(b)(1).*

[43] *Cybersecurity Act of 2015 (CISA), Section 104(e)(1), (2).*

[44] *National Insider Threat Task Force, Insider Threat Program Maturity Framework, November 1, 2018. Available at https://www.dni.gov/files/NCSC/documents/nittf/20181024_NITTF_MaturityFramework_web.pdf*

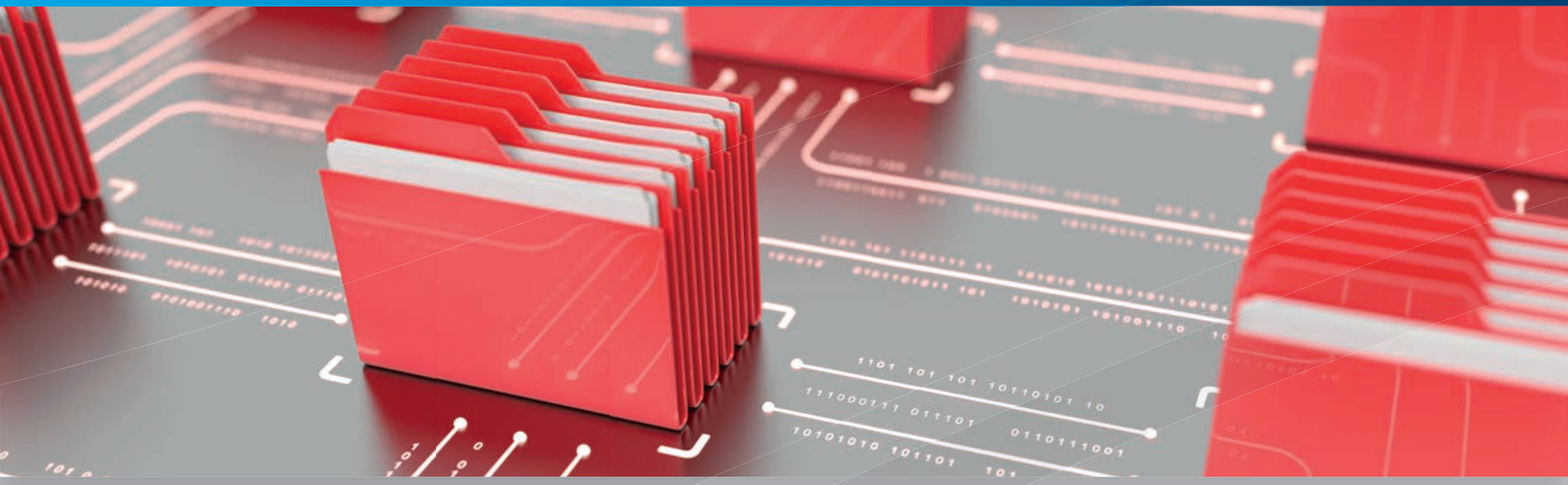
[45] *Roberts v. United States, 445 U.S. 552, 558 (1980); see also Ed Rachal Found. v. D'Unger, 207 S.W.3d 330, 333 (Tex. 2006) ("Both employers and employees have civic and social obligations to report suspected crimes.")*

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit trade association dedicated to advancing collaborative, public-private approaches to intelligence and national security priorities. Through the application of industry expertise, leading-edge academic research and commercial best practices, INSA seeks to make the Intelligence Community more effective and efficient. Our 160+ member organizations and its 4,000+ individual and associate members include senior executives and intelligence experts in the public, private and academic sectors.

ABOUT INSA'S INSIDER THREAT SUBCOMMITTEE

INSA's Insider Threat Subcommittee researches, discusses, analyzes, and assesses counterintelligence and insider threat issues that affect government agencies, cleared contractors, and other public and private sector organizations. The Subcommittee works to enhance the effectiveness, efficiency, and security of government agencies and their industry partners, as well as to foster more effective and secure partnerships between the public, private and academic sectors.



INSA
INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Building a Stronger Intelligence Community

(703) 224-4672 | www.INSAonline.org