The "T" Factor and Cleared Industry

by Stanley L. Sims and William D. Stephens

"Some men see things as they are and ask why. Others dream things that never were and ask why not."

- George Bernard Shaw

This article focuses upon threat—the "T" factor—and presents three conditions necessary to more fully include threat in the management of risk in cleared industry, with a goal of providing a "way ahead" for taking the initiative back from foreign collection entities. The three conditions are: a common understanding of risk; new expectations for cleared industry; and new expectations for U.S. government support to cleared industry.

THE CHALLENGE

"Things as they are," the current situation with regard to the crown jewels in our nation's treasure—sensitive or classified[1] information and technologies resident in the U.S.-cleared industrial base—is that they are in great danger: the classified materials are at risk, while the sensitive but unclassified materials are being stolen, lost, or compromised at an alarming rate. The Federal Bureau of Investigation is kept sufficiently busy with espionage cases generated from the Defense Security Service (DSS), and industry efforts to protect these materials have proven to be extremely worrisome. Every year the National Counterintelligence Executive, currently Robert "Bear" Bryant, conducts a review of the efforts of every U.S. government counterintelligence activity. He always asks the same question: "Are we winning?" The answer, with regard to the protection of sensitive or classified information and technology in the U.S.-cleared industrial base, is, if not "NO!", then at least "Not yet!" (Editor's Note: Recent reports indicate Mr. Bryant was scheduled to retire at the end of January 2012.)

Mr. Bryant recently stated that "[T]he future of U.S. national security is located in the facilities and I.T. networks of cleared defense contractors; these assets are undoubtedly high on the target list of many foreign intelligence services." The DSS trend analysis of reporting from defense industry, as well as analysis from the Office of the National Counterintelligence Executive, demonstrates that the threat to industry is growing and threatens the U.S. economy. These potential losses of sensitive economic information and technologies represent significant costs to U.S. national security. In fiscal year 2010, the Defense Security Service witnessed a stunning 140 percent increase in the number of suspicious reports being submitted by cleared contractors that were determined to be of intelligence value. Making this problem more daunting is the sheer size and diversity of the cleared defense industry, with more than 8,500 companies operating some 13,300 cleared contractor facilities and employing roughly 1.2 million people. While counterintelligence is still at its core a human issue, globalization and our dependency on information technology systems mean that the risk landscape has dramatically changed, as evidenced by foreign cyber spies' successful penetration of cleared contractor unclassified systems. Clearly, the long-standing security rules, regulations, and approach are no longer enough to protect against the trusted insider and more complex hostile foreign collection efforts—most specifically with regard to protecting sensitive information on industry's unclassified networks.

Admittedly, definitive proof of the scope of the loss is hard to produce. That difficulty stems at least partly from the embarrassment that such losses cause, whether responsibility for safeguarding those crown jewels falls to cleared industry or the U.S. government in any particular case. However, public reports of losses to the F-35, F-22, P-8, and other programs provide clear evidence that the decades-long effort to "control the initiative" in the struggle between foreign collection entities and the U.S. government has not gone well. A recent CNN report in response to the Defense Security Service's publication *2011 Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry* called the reported findings "alarming"—and reported numbers for the subsequent year, while not fully analyzed, appear to have doubled.

At its most fundamental level, the U.S. government is the customer and end user of the classified programs, technologies, equipment, and services produced and

delivered by cleared industry. However, in this business-consumer relationship, the customer—the U.S. government—assumes the negative consequences when a compromised product is delivered. Therefore, the counterintelligence, security, and acquisition communities, from the senior-most program executive officers down to entry-level specialists, must understand the very real threats posed to our sensitive or classified information and technology, make informed decisions as a result of those threats, and ensure that there is increased accountability for uncompromised products across the acquisition lifecycle.

[I]n many instances, relevant threat data are not reaching key decision-makers. [T]hose decision-makers cannot make informed decisions when "they don't know what they don't know."

This is not to imply that government or cleared industry is turning a blind eye to the threat. Many are doing the best they can with the protection standards, threat information, and resources currently available; it is clear that most in the U.S. government and industry have the interests of the nation at heart when they make decisions. The problem is that, in many instances, relevant threat data are not reaching key decision-makers. Put another way, those decision-makers cannot make informed decisions when "they don't know what they don't know."

To reach the goal of Shaw's dream—of "things that never were," but might be—will require the U.S. government to take back the initiative from the foreign entities that steal our national secrets. The Defense Security Service plays a key role—probably *the* key role—in assisting cleared industry. Can DSS be better leveraged to perform its oversight function? This article proposes that the answer is "Yes"—but it depends on DSS adopting a more robust approach to managing risk in cleared industry.

Such an approach must more completely consider threat—the "T" factor—than has been the case heretofore.

THE DEFENSE SECURITY SERVICE MISSION AND LEGACY

The Defense Security Service, on behalf of the Department of Defense and other U.S. government departments and agencies, supports national security and the warfighter through its security oversight and education missions. DSS oversees the protection of U.S. and foreign classified information and technologies resident in the U.S. cleared industrial base under the National Industrial Security Program, and it serves as the Department's functional manager for the education, training, and professional development of security professionals for DoD, other U.S. government personnel and, by default, cleared industry.

As a result of its mission, the Defense Security Service is ultimately in the risk management business, as it relates to safeguarding sensitive or classified information and technology resident in cleared industry. For this discussion, risk will be defined as a function of threat, vulnerability, and value (i.e., the value of the technology/information being targeted).

Legacy practice has been to approach the management of risk by focusing on vulnerability. DSS carried out its oversight responsibilities by, in effect, requiring cleared industry to build a wall between the U.S. classified information/technologies in its charge and those attempting to steal them. Cleared industrial facilities were then inspected for compliance with the National Industrial Security Program's *Operating Manual*. However, this legacy practice offered little consideration of either threat or value in managing risk, and it was established before cyber espionage redefined the nature of "the wall." Today's DSS leadership views as critical to the management of risk the consideration of not just the vulnerability variable, but of threat and value as well, and is adjusting its practices accordingly – we must stay in front of the threat and NOT behind the vulnerability!

The aforementioned three conditions necessary to more fully include threat—the "T" factor—in the management of risk in cleared industry are: a common understanding of risk; new expectations for cleared industry; and new expectations for U.S. government support to cleared industry.

RISK AND THE "T" FACTOR

If the U.S. government and cleared industry together are to "take back the initiative," they must have a common understanding of the "T" factor and how it relates to risk management. While the finer points of different risk equations are debatable, the general equation given above—that risk is a function of threat, vulnerability, and value—is sufficient for understanding that threat is a key and integral element in managing risk. Risk cannot be managed without considering threat.

The Defense Security Service's vulnerability-centric legacy approach primarily addressed the "T" factor only in the reporting of suspicious incidents. DSS was not properly equipped to analyze threats, understand their depth and breadth, refer them for action, or track them to resolution.

The legacy approach, as required by the National Industrial Security Program, focused on protecting classified information and technology and determining whether the security "wall" it required of cleared industry met the standards intended to do so. It seemingly relied on the premise that a wall built to standards must be essentially impermeable—the industrial espionage equivalent of Maginot Line thinking. The National Industrial Security Program standards did not consider those who might be attempting to penetrate the wall or, worse yet, had already penetrated it. Unfortunately, history demonstrates the "impermeable wall" theory to be ludicrous, since spies have penetrated even the well-secured organizations within the U.S. government. Plus, more and more valuable, sensitive, but unclassified information and technology currently reside outside the wall. And the problem is now even more complex, as this once "impermeable" wall now extends well into the unsecure virtual realm of the cyber domain, an area already proven to be ripe for exploitation.

INCREASED "T" FACTOR EXPECTATIONS FOR CLEARED INDUSTRY

"Taking the initiative" and preventing the loss of critical defense technology and information will require a true public-private team effort. Undoubtedly, the Defense Security Service, the U.S. Intelligence Community, and federal law enforcement agencies face a challenging task in assisting cleared industry to better understand and mitigate the threat to its sensitive/unclassified and classified systems, technologies, and information. There are actions both the Defense Security Service and cleared industry can take to "step up their game," with greater capacity and capability focused upon the threat variable of the risk management model.

The Defense Security Service credits industry for what it has accomplished in protecting classified information and technologies under the existing National Industrial Security Program. However, over the last two years, the Defense Security Service has accentuated to industry this necessity for both parties to "step up their game," and industry's response has clearly contributed to significant increases in the number of suspicious incident reports, federal investigations of known or suspected penetrators of the cleared industrial base, and improved mitigation of security vulnerabilities. In our dialogue with industry we have offered the following three key perspectives that we believe have the potential to further increase industry's capability in the "T" factor arena:

(1) *Threat management capability*: Develop and field an internal threat management capability staffed with "risk professionals" (we feel this is a more appropriate title for today's multi-disciplined security personnel) who are skilled, agile, and thoughtful in understanding all elements of the risk equation and applying each variable to their company and the protection of U.S. information in their hands. Key requirements of industry risk professionals should include knowledge of the following: the threat posed to U.S. sensitive or classified information and technology resident in their companies; U.S. government threat reporting requirements and an internal system for aggregating company reporting to develop a comprehensive threat picture; and the value of the technologies being targeted and the consequences of their loss. A successful model has been the creation of a single corporate point of command and control for risk, particularly for receiving and reporting threat information, and accountable for knowing the risk to all sensitive or classified information and technology in the company's charge.

(2) *Reporting*: The foundation of the analytical products developed by the Defense Security Service to inform industry of the threat is the timely and accurate reporting by the cleared contractor community of security vulnerabilities and illicit collection attempts. Yet, only ten percent of cleared contractors fulfill suspicious incident reporting required by the National Industrial Security Program *Operating Manual*; an even smaller portion of industry—approximately three percent—reports cyber-related events. Undoubtedly, there are many who are not reporting what they should, in some instances because they lack knowledge of reporting requirements, in others because of competing priorities and interests. The result is that both industry and the U.S. government have an incomplete threat picture, and thus an imprecise understanding of the true threat posed by foreign intelligence entities targeting U.S. technological secrets. All U.S. industry, particularly those companies operating under the National Industrial Security Program, must cultivate a culture of reporting—not only is it a requirement; it is also a national security imperative.

DSS has also launched a "Partnership with Industry" program to improve our relationship with industry and to identify best practices. These and other innovative approaches will strengthen our partnership and contribute to "taking back the initiative."

(3) *Partnership*: Continue to strengthen the partnership with the Defense Security Service and other U.S. government entities in all aspects, but particularly in the "T" factor lane. DSS and industry share a mutual goal—preventing the loss of our nation's critical assets—and our

successes (and failures…) are inextricably intertwined. The approach must be proactive and innovative in identifying and articulating the threat to industry partners. The recent response from industry has been excellent, with several new DSS threat products having been developed as a result of industry interests, including company-specific threat assessments (*Gray Torch*, now produced jointly with corporate partners); program-specific threat assessments (*Bronze Dragon*); and industry cyber threat publications. DSS has also launched a "Partnership with Industry" program to improve our relationship with industry and to identify best practices. These and other innovative approaches will strengthen our partnership and contribute to "taking back the initiative."

Both the Defense Security Service and cleared industry are committed to working together to identify threats and vulnerabilities and mitigate them until an acceptable level of risk is achieved. The objective of DSS, then, whether in reality or perception, cannot be to catch cleared industry in a failing security posture during an inspection in order to administer punishment. Likewise, the sole objective of cleared industry cannot be to pass the inspection process while leaving vulnerabilities that are or could be exposing sensitive or classified information and technology to risk of exploitation by foreign intelligence entities. Neither the U.S. government nor cleared industry can ignore an "unacceptable risk."

INCREASED EXPECTATIONS FOR GOVERNMENT SUPPORT TO CLEARED INDUSTRY

How can we support and enable industry so that it is sufficiently informed of threats to be able to protect and defend its companies and deliver uncompromised products? No other organization is better positioned than the Defense Security Service to assist cleared industry in protecting sensitive or classified information and technology in its possession. The approach is three-fold: (1) We must make sure industry is able to receive classified threat information; (2) We must help instill a threat-responsive culture throughout industry; and (3) We must develop and implement clear policies which hold both government and industry responsible for delivering uncompromised products, with incentives for success and consequences for failure that have genuine deterrent value.

(1) *Receiving threat information*: Information sharing as a problem has received enormous attention since the events of September 11, 2001. Resolving it has proven to be terribly complex, revealing the challenges posed by the size and scope of our government. The U.S. government must clarify authorities, continue to improve and refine its information-sharing business practices, and provide enhanced tools and the right equipment to enable industry to expeditiously receive and transmit classified threat information. Yet, as to technical and administrative aspects, solving the information-sharing problem should be a relatively simple and straightforward matter for DoD and industry. Industry lacks the secure communications equipment and necessary authorities to transmit and receive classified threat information. (While a few facilities can transmit secret information via the Secret Internet Protocol Router Network (SIPRNet), these systems are provided by specific programs and are not set up to process classified threat information.) The continuation of an Industrial-Age approach to an Information-Age problem is simply unconscionable in the 21st century.

The culture must change from one in which companies fear exposure of their internal vulnerabilities to one in which they voluntarily share where they are most vulnerable based on identified threats.

The Defense Security Service already possesses the authority to plan and execute a modern program that will enable industry to receive the requisite threat information. It can select and sponsor companies to procure and install secure, dedicated communications equipment and thereby to receive classified threat information. DSS can conduct field trials of this capability in larger companies when resource and policy constraints allow. The question is whether the up-front costs associated with fielding the capability for industry to send and receive classified threat information is a much lesser evil than the costs of our "national treasures" being lost, stolen, and compromised. (Once this capability is fully fielded, it will open up a classified communications channel to cleared industry that would be useful to the Department of Homeland Security, the Federal Bureau of Investigation, and other agencies which might provide classified threat information to industry.)

(2) *A threat-responsive culture*: In addition to receiving classified threat information, industry must be able to recognize the value of the information and know what to do with it. The Defense Security Service is moving forward with efforts to create a "threat course" for industry, designed to educate industry as well as government security professionals as "threat professionals." As the paradigm continues to shift away from the vulnerability-only approach, a professional cadre of threat professionals must

be available to recognize and mitigate threats in both the physical and cyber domains, and know how and when to report this information. As this program comes to fruition, these certified threat professionals will be recognized as subject matter experts within their companies for both vulnerability and threat, and will guide business decisions with due consideration given to threat, cost, schedule, and performance. Complementing this is the Defense Security Service's efforts to continuously improve the quality of security, i.e., vulnerability, training already offered to both government and industry.

Yet, a threat course and enhanced security training are not enough. We must incentivize companies to be proactive in their security and counterintelligence efforts. The culture must change from one in which companies fear exposure of their internal vulnerabilities to one in which they voluntarily share where they are most vulnerable based on identified threats, and are recognized for identifying those weaknesses and rewarded for partnering with the Department of Defense to apply fixes.

(3) *Responsibility for uncompromised products*: The challenge will be providing the necessary support to industry in the threat arena, while simultaneously holding industry accountable for delivering uncompromised goods and services. "Things as they are" allow companies to use strict adherence to the National Industrial Security Program as the singular benchmark for measuring their ability to safeguard the sensitive and classified information in their charge, but even the most sound, industrial security-compliant program is insufficient if due consideration is not given to threat. Certainly, the U.S. government can amend policies to require that more emphasis be given to threat—and we are moving in that direction—but until the culture shifts within government and industry to the point where both recognize the value of threat information, changing the policy will not matter.

Managing risk—both threat and vulnerability—is not an endeavor without costs. Nevertheless, even in today's shrinking budget environment, it is still worth doing. Distributing these costs across the government and industry sectors will require an enhanced partnership conducted with skill and agility. Larger companies may need to take a lead role in the effort by supporting smaller subcontractors, while the U.S. government must also explore ways to shore up smaller companies that need assistance in certifying their ability to manage risk as part of the supply chain. Notwithstanding the patriotic motivation to "do the right thing," the immediate returns on investment which corporate shareholders demand and the short budget cycles to which we must answer mean that anything that increases overhead, even with the potential to deliver long-term savings, is difficult to get off the ground. But we must try.

CONCLUSION

The reasons the struggle to protect America's "crown jewels" has not been going well for those charged with protecting them are many, and infinitely debatable. Such debates may be relevant to those charged with assigning blame for past losses. However, settling such questions is not necessary for those focused on taking back the initiative in the future.

Current government processes place much of the responsibility for considering threat and vulnerability on security and counterintelligence professionals. In many instances, these security/risk professionals, whether employed by the U.S. government or industry, serve in support and advisory roles and lack the ability to make or seriously influence key decisions. Senior government and industry leaders must more seriously consider threat and vulnerability in their business decisions. They must: recognize the unabated, indeed growing, threat that foreign intelligence entities pose to our industrial base in both the classified and unclassified realms; develop their own capabilities in managing risk, particularly regarding the "T" factor; and support sound policies which incentivize success and have consequences for those who wittingly allow our sensitive and classified information and technologies to be lost, stolen, or compromised before they are delivered.

Until the acquisition, security, and counterintelligence communities fully recognize the "T" factor in their policies and resource allocations and provide industry with the support it needs to recognize and mitigate threat, it will not matter how tall or how wide we require industry to build the wall—the wall *will* be penetrated, and our national treasures *will* continue to be stolen.

(Authors' Note: The opinions expressed herein are those of the authors, and are not necessarily the official views of, or endorsed by, the U.S. Government or the Department of Defense. Defense Security Service products are available at http://www.dss.mil/isp/count_intell/index.html.)

Notes

[1] The Defense Security Service is chartered to oversee the protection of U.S. and foreign classified information in the hands of industry under the National Industrial Security Program (NISP). While the NISP only considers classified information, other information controlled by the U.S. government, particularly sensitive unclassified information which may have military, intelligence, or other implications for national security, is also of concern. In many instances, the aggregate of this sensitive unclassified information is of equal value to classified information, and places national security at risk if compromised.

Stanley L. "Stan" Sims, a member of the Defense Intelligence Senior Executive Service (DISES), was appointed Director of the Defense Security Service (DSS) on December 5, 2010. Prior to this, Mr. Sims was the Director of Security for the Department of Defense, Office of the Under Secretary of Defense for Intelligence. As such, he was the senior DoD security official responsible for the development, implementation, and oversight of national- and department-level security policies. He is a retired Army MI officer and decorated combat veteran with more than 32 years of distinguished military and federal service. His awards include the Presidential Rank Award, Bronze Star Medal, Defense Superior Service Medal, and the Legion of Merit. A native of Arkansas, Mr. Sims holds a BS degree from Arkansas State University, and master's degrees in Administration from Central Michigan State University and in National Security Strategy from the National Defense University.

William D. Stephens, a member of the DISES, has been the Director of Counterintelligence, DSS, since August 2009. Prior to his DSS assignment, Mr. Stephens had a distinguished military career, serving in a variety of progressively responsible leadership positions as a special agent and senior field commander with the U.S. Air Force Office of Special Investigations (AFOSI). He retired from the Air Force in 2009 after completing a tour as the commander of all AFOSI forces in Europe. He is the recipient of numerous military decorations, including the Defense Superior Service Medal. Mr. Stephens received a BS degree from Auburn University and has earned three MA degrees from Central Michigan University, the Naval Postgraduate School, and the National Defense University, respectively.