

SEPTEMBER 2019



NSI

THE NATIONAL SECURITY INSTITUTE
At George Mason University's Antonin Scalia Law School

CRITICAL ACCESS: **ENHANCING THE VALUE OF PRIVATE SECTOR SECURITY CLEARANCES TO PROTECT CRITICAL INFRASTRUCTURE**

By Jenny Menna¹

NSI LAW AND POLICY PAPER

CRITICAL ACCESS: ENHANCING THE VALUE OF PRIVATE SECTOR SECURITY CLEARANCES TO PROTECT CRITICAL INFRASTRUCTURE



THIS NSI LAW AND POLICY PAPER:

1

Describes the development of programs providing high-level clearances to critical infrastructure industry representatives to facilitate information sharing around growing nation state threats.

2

Evaluates the current gaps and inconsistencies among these clearance programs.

3

Argues that information sharing at classified levels is essential and critical infrastructure clearance programs must be enhanced.

4

Provides recommendations to ensure clearance programs are facilitating actionable information sharing and a secure critical infrastructure.



CONTENTS

02 EXECUTIVE SUMMARY

05 BACKGROUND ON CRITICAL
INFRASTRUCTURE CLEARANCES

08 KEY ISSUES AT STAKE

09 AUTHOR'S VIEWS

10 ACTIONABLE RECOMMENDATIONS

11 CONCLUSION



» Background On Critical Infrastructure Clearances

PROTECTING CRITICAL INFRASTRUCTURE

In 2006, the Department of Homeland Security (DHS) began sponsoring security clearances for private sector critical infrastructure representatives to more fully assess risk and take protective actions.

While initially focused on the threats posed by Al Qaeda and other terrorist organizations, nation state threats began to emerge more significantly and drew focus on the intersection of national security, economic security, and cybersecurity.

A HEIGHTENED RESPONSE

In response, the Bush Administration created the Comprehensive National Cybersecurity Initiative (CNCI), which focused on securing defense, classified, and federal civilian networks in an effort to “stop the bleeding.”

The final component of CNCI (dubbed Project 12 as the 12th of 12 initiatives) recognized that the vast majority of critical infrastructure is owned and operated by the private sector, and recommended providing high level clearances to a set of industry points of contact at the Top Secret / Sensitive Compartmented Information (TS SCI) level.

» Key Issues At Stake

UNEVEN AGENCY PROGRAMS

Because DHS’ critical infrastructure protection programs are driven by an assigned Sector Specific Agency, the quality of program participation, content, and depth varies greatly. The partnership between the Department of Treasury and the financial sector is more mature, well-resourced, and advanced than programs for other critical infrastructure sectors.



UNEVEN PARTICIPANT EXPERTISE AND PARTICIPATION

Private sector participants vary greatly, from mid-level corporate information security operators, to association and ISAC staff, to C-suite level executives of critical infrastructure firms. Their use of granted clearances varies just as much.

PATCHY SYSTEM PERPETUATES RISK

These discrepancies could result in a gap in the government's understanding of the risk landscape, or in a company not obtaining timely information or having information received by an individual without the proper role or function to take action.

Ultimately, the government may be providing clearances for the wrong individuals, while not providing clearances for those who could add greater value.



Author's Views

CLEARANCES REMAIN CRITICAL TO CYBERSECURITY

As the private sector has increasingly been targeted by nation state actors and much of the threat data comes through signals intelligence, information must continue to happen at classified levels.

THE PRIVATE SECTOR CLEARANCE PROGRAM NEEDS REVIEW AND ENHANCEMENT

The Private Sector Clearance Program referenced in CNCI Project 12 has added significant value to cybersecurity for industry, but now is the time to increase the consistency and clarity of security clearance and classified information sharing programs to further reduce risk.

ACTIONABLE INFORMATION SHARING IS THE ULTIMATE OBJECTIVE

Clearances are a means to help inform critical infrastructure protection activities, and agency programs should be reviewed and improved to better achieve this objective.



Actionable Recommendations

1

REVIEW CLEARANCES

DHS should review all permanent clearances at the Secret and TS SCI level to fill gaps, and ensure appropriate clearance levels—enabling better information sharing, security outcomes, and decision making.

2

ADOPT BEST PRACTICES

DHS should evaluate best practices in both granting and utilizing clearances across sectors to identify gaps and opportunities for efficiency and improvement.

3

INITIATE NEW PROJECT 12

DHS should consider a full review of Project 12 to benchmark progress, guide recommendations and milestones for improving cybersecurity information sharing, and collaboration with critical infrastructure—including state and local governments—at all levels of classification.

BACKGROUND ON CRITICAL INFRASTRUCTURE CLEARANCES



» Protecting Critical Infrastructure

CRITICAL INFRASTRUCTURE CLEARANCES

- In 2006, the Department of Homeland Security (DHS) began sponsoring security clearances for a small number of private sector critical infrastructure representatives.²
- Private sector individuals have long-received security clearances as employees of cleared defense or civilian contractors through the procurement process, as a term of the contract for supporting functions.
- The DHS program differs significantly as clearance is not linked to contract performance, but rather to enable critical infrastructure owners and operators (and some of their representatives such as Information Sharing and Analysis Center staff) to more fully assess risk and take appropriate protective actions for their respective companies and industries.

EVOLUTION OF THE THREAT

- The initial clearances were offered with a focus on the potential physical security threats posed by Al Qaeda and other terrorist organizations, in keeping with DHS' founding impetus.³
- In the final years of the Bush Administration, a new threat vector gained prominence: Chinese intrusions into federal defense and civilian agency networks, as well as cleared defense contractors' networks.⁴
- Large quantities of intellectual property were also being exfiltrated from America's and our allies' networks⁵—drawing focus on the intersection of national security, economic security, and cybersecurity.



A Heightened Response

THE COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE

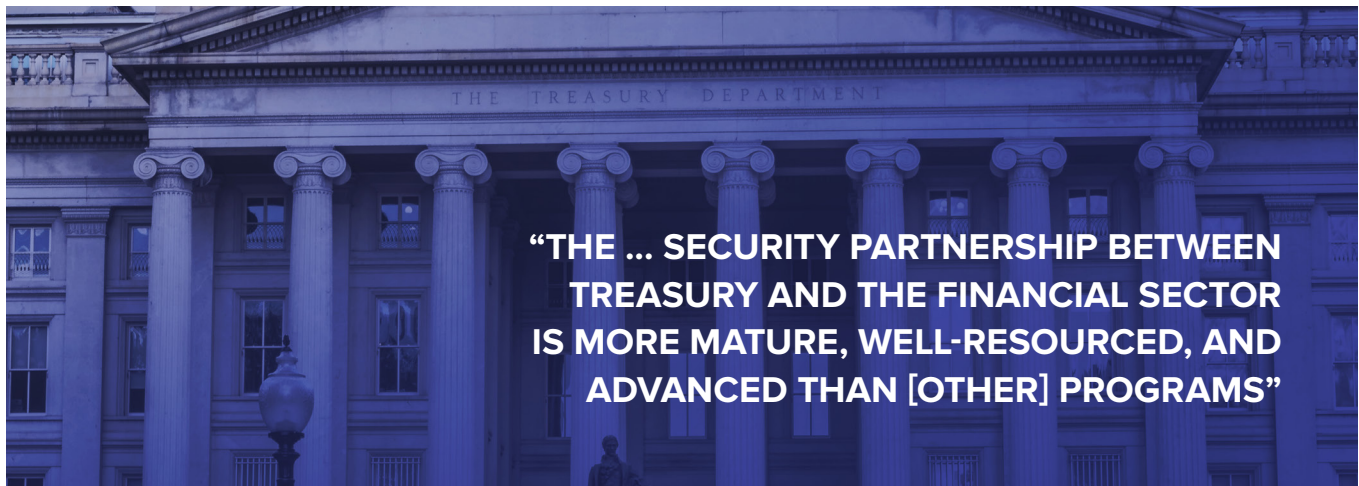
- In response, the Bush Administration created the Comprehensive National Cybersecurity Initiative (CNCI) under National Security Presidential Directive 54 / Homeland Security Presidential Directive 23.⁶
- CNCI launched a coordinated, interagency effort, including defense, intelligence, law enforcement, and homeland security players.⁷
- CNCI, and the majority of its efforts, focused on securing defense, classified, and federal civilian networks in an effort to “stop the bleeding” from the Chinese intrusions.

CNCI PROJECT 12

- The final component of CNCI (dubbed Project 12 as the 12th of 12 initiatives) recognized that the vast majority of critical infrastructure is owned and operated by the private sector, and that government must work with industry to help industry defend itself from an evolving set of cyber risks. This initiative was officially entitled, “Define the Federal role for extending cybersecurity into critical infrastructure domains.”⁸
- Project 12 directed DHS to create a report on improving critical infrastructure cybersecurity. The completed report, developed with extensive private sector input, created a list of deliverables and milestones for government focused on improved information sharing and piloting new approaches to partnership and collaboration, at the classified and unclassified level.⁹
- **Private Sector Extended Higher-Level Clearances.** One recommendation tasked DHS to test providing access and sharing data with a very small set of industry points of contact at the Top Secret / Sensitive Compartmented Information (TS SCI) level—a highly restricted category of classified information.¹⁰
 - The goal for these higher-level clearances was two-fold.
 - First, these experts could help government to craft messages that would resonate with, and enable action by, the private sector based on their understanding of how industry actually operates. Their individual gravitas would also help to convey that the government information provided really was important and therefore drive action.
 - Second, government recognized the lack of expertise in industry operations in house, and needed assistance understanding and assessing risk, steering intelligence requirements, and communications.
 - President Obama formalized the program in 2010 by signing Executive Order 13549, “Classified National Security Information Program for State, local, tribal, and Private Sector Entities”—otherwise known as the

Private Sector Clearance Program.¹¹ He then expanded the program in 2015 with Executive Order 13691, “Promoting Private Sector Cybersecurity Information Sharing.”¹²

- DHS’ Private Sector Clearance Program for Critical Infrastructure now has a mature centralized administrative operation, and hundreds, if not a few thousand, of industry representatives have been cleared (statistics not available).
- **C-Suite Gets Read In.** In addition to regular, ongoing information sharing with private sector cybersecurity professionals, specific and critical cyber threats required DHS to team with intelligence community leaders to “read in” hundreds of industry executives at the SCI level.
 - Because the SCI clearance process is highly time consuming and requires extensive reporting and investigation, permanent clearances were not practical for these key C-suite executives.
 - In addition to some individual meetings sponsored by the Office of the Director of National Intelligence (DNI), DHS partnered with the National Security Agency (NSA) for focused, and broader engagement across several sectors. These briefings on threat were paired with specific recommendations for mitigation.
- **Treasury Stands Out.** The clearances, information sharing, and overall security partnership between the Department of Treasury and the financial sector is more mature, well-resourced, and advanced than programs for other critical infrastructure sectors.
 - Treasury has accomplished this by resourcing staff to support clearance justification review and to identify and shape content and agendas for monthly classified briefings connected via Secure Video Teleconference for financial industry cybersecurity leaders nationwide through FBI field offices.
 - Treasury also schedules larger in-person briefings 3 times per year, more strategic in nature, in tandem with its Sector Coordinating Council meetings.
 - Treasury facilitated briefings also include regular SCI level presentations, as several large financial sector firms have TS SCI cleared staff. Some of these clearances leveraged the large number of previously cleared government experts departing for the industry, while others were provided to firms designated on the “Section 9” list of most critical infrastructure.¹³



KEY ISSUES **AT STAKE**



» Uneven Agency Programs

- Because DHS' critical infrastructure protection programs are aligned according to critical infrastructure sector, and each sector's clearance list and classified briefing schedule and content is driven by an assigned Sector Specific Agency, the quality of program participation, content, and depth varies greatly.
- Treasury has developed extensive, regular clearance processing, and classified briefing cadences.
- However, other agencies' programs are less robust and they and their sector companies' resources, priorities, threats landscapes, and capabilities vary significantly.

» Uneven Participant Expertise and Participation

- The roles, expertise, and function of the private sector participants vary greatly, from mid-level corporate information security operators, to association and ISAC staff, to C-suite level executives of critical infrastructure firms.
- The reason, mechanism, and frequency that these individuals use their clearances, if they do, varies greatly as well.
- That said, the author has found no evidence to date that classified sharing with critical infrastructure partners at any level has resulted in risk to our national security.

» Patchy System Perpetuates Risk

- As the threat landscape continues to evolve, program results and participation vary greatly between sectors and even within a single industry.
- These discrepancies could result in increased risk where a company may not obtain timely, actionable information for protection, or that information may be received by an individual without the proper role or function to take action.
- These discrepancies could also result in a gap in the government's understanding of the risk landscape of an industry or operator of a critical function.
- Ultimately, the government may be providing clearances for the wrong individuals—those who provide low value in this process—while not providing clearances for those who could add greater value. Clearances are expensive and time consuming.

AUTHOR'S VIEWS



Clearances Remain Critical To Cybersecurity

- As the cyber threat landscape has evolved, the private sector has increasingly been targeted by nation state actors.
- From Chinese theft of intellectual property to drive its economic development, to Iranian Distributed Denial of Service attacks on banks in retaliation for U.S. sanctions, to the North Korean destructive malware attack on Sony and more recently attributed attacks aiming to finance its regime, private companies face attacks in cyberspace not just from criminals but from foreign regimes.
- As much of the threat data has come through signals intelligence channels and remained highly sensitive, information sharing has and must continue to happen at classified levels.



The Private Sector Clearance Program Needs Review and Enhancement

- The Private Sector Clearance Program referenced in CNCI Project 12 has added significant value to cybersecurity for industry, but now is the time to increase the consistency and clarity of security clearance and classified information sharing programs to further reduce risk.
- CNCI Project 12 intended for the industry SCI clearances to be issued as a pilot. Now is the time to review who has clearances, including their level, how often they are used (briefings attended), and how participants are able to leverage that information in a way that meaningfully improves critical infrastructure security.
- Identifying best practices and areas for improvement can be used to increase consistency and clarity in agency clearance programs and further reduce risk for critical infrastructure companies, as well as for government in only sharing sensitive information with those with a true “need to know.”
- The Treasury program, though not perfect, offers strong best practices that could be replicated.



Actionable Information Sharing Is The Ultimate Objective

- Clearances are only a means to an end—sharing actionable threat information with industry and enabling industry experts to help inform government critical infrastructure protection activities.
- DHS should conduct a study of classified threat sharing across sectors, identify best practices and areas for improvement, and work with the designated Sector Specific Agencies to improve the programs and increase consistency.

ACTIONABLE RECOMMENDATIONS



1 REVIEW CLEARANCES

REVIEW ALL EXISTING CLEARANCES TO IDENTIFY GAPS AND PRIORITIES

- DHS should review all permanent clearances at the Secret and TS SCI level to fill gaps and ensure appropriate clearance levels based on role and expertise of the individual, the firm's place or critical function within industry, and engagement in broader security initiatives. This will enable more effective decision making both within individual firms and by the government.
- DHS should also work with the ODNI and Director of NSA to create a process and program for "read ins" for C-level executives to drive significant investment and influence corporate decision making, which can only be done from the highest levels, to address critical threats.

2 ADOPT BEST PRACTICES

ADOPT BEST PRACTICES FOR CLEARANCE PROCESSING AND UTILIZATION

- DHS should thoroughly evaluate best practices in both granting and utilizing clearances across the sectors to identify gaps and opportunities for efficiency and improvement, and work with Sector Specific Agencies to create a more effective national effort in support of the National Critical Function activity.

3 INITIATE NEW PROJECT 12

DEVELOP THE NEXT PROJECT 12 REPORT TO ADDRESS TOMMOROW'S SECURITY NEEDS

- DHS should consider a full review of the 2008 Project 12 report as a baseline of cybersecurity engagement with critical infrastructure and benchmark progress on its recommendations. The report addressed areas for improving information sharing and collaboration far beyond clearances and classified sharing.
- A new report should include recommendations and milestones for improving cybersecurity information sharing and collaboration with critical infrastructure—including state and local governments—at all levels of classification.
- Much work was done during the Bush, Obama, and Trump Administrations, but there is much more to be done in this mission space given evolution in threats, technology, and government and industry capabilities.

CONCLUSION



The Private Sector Security Clearance Program and classified information sharing briefing efforts have resulted in significant positive results for our nation's critical infrastructure cybersecurity and helped to improve government intelligence requirements and focus mitigation efforts. It is impressive that the trust shown to industry representatives has been maintained and that classified data has not been compromised. However, between changes in leadership and Administrations, and differences born of sector-driven implementation, benefits have not necessarily been consistent or maximized.

Due to other priorities, no formal and comprehensive reassessment of the CNCI Project 12 recommendations to include clearances and classified sharing has taken place. The creation of CISA and launch of the National Critical Function Initiative¹⁴ provides an excellent opportunity for a review to leverage successes more broadly, improve upon areas of weakness, and drive meaningful progress in critical infrastructure cybersecurity for the next decade.

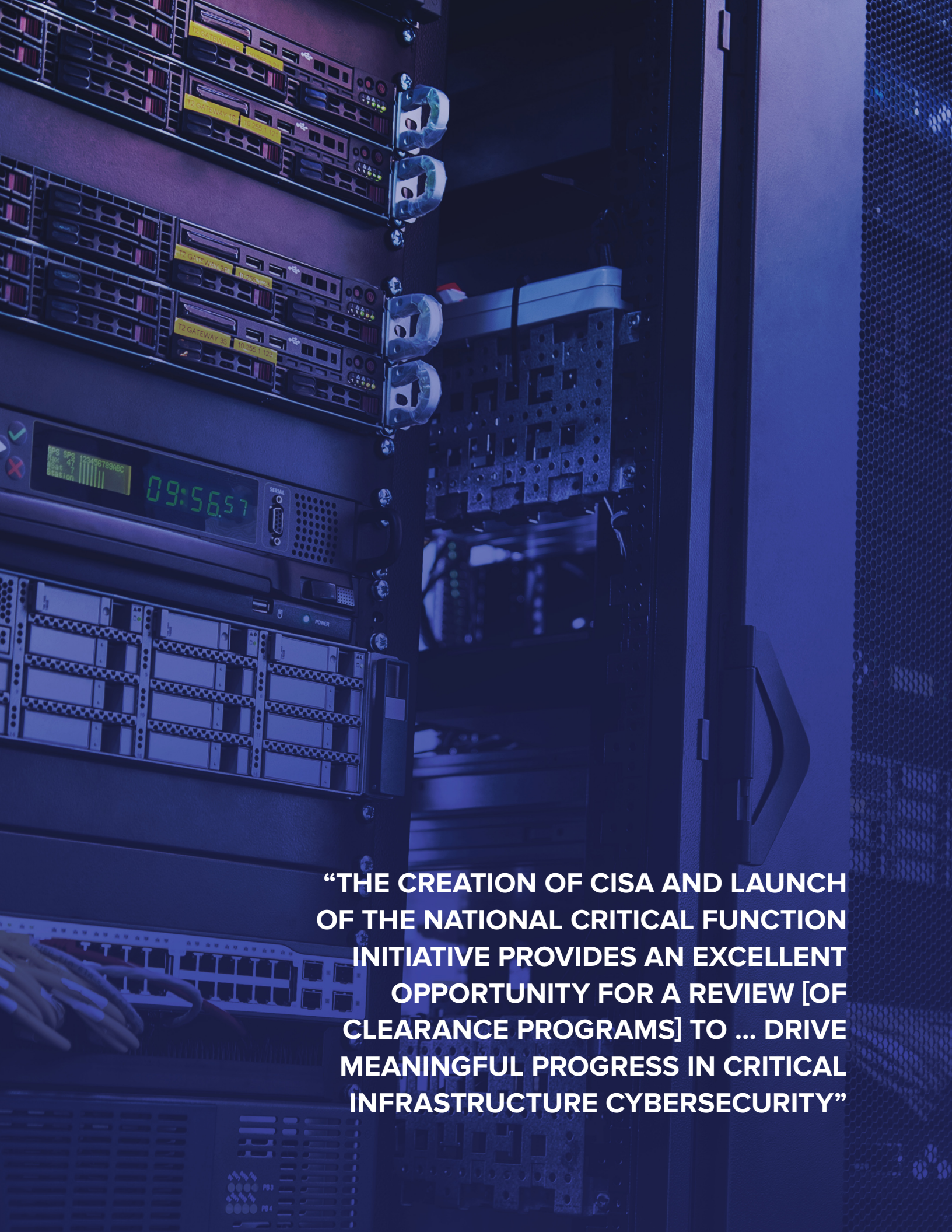
The author recommends a joint effort for the review, report, and recommendations similar to the approach taken to developing the Project 12 report—leveraging the DHS Critical Infrastructure Protection Advisory Council mechanism and authorities to include broad expertise and enable the most innovative and effective solutions.



**“CLEARANCES ARE ONLY A MEANS
TO AN END—SHARING ACTIONABLE
THREAT INFORMATION WITH INDUSTRY
AND ENABLING INDUSTRY EXPERTS TO
HELP INFORM GOVERNMENT CRITICAL
INFRASTRUCTURE PROTECTION ACTIVITIES.”**

ENDNOTES

- 1 Jenny Menna is a Visiting Fellow at the National Security Institute at the Antonin Scalia Law School at George Mason University. Ms. Menna is currently the Senior Vice President and Cybersecurity Partnership Executive at U.S. Bank. Ms. Mena previously held a variety of Senior Executive Service positions in the Department of Homeland Security (DHS) component responsible for securing federal civilian, state and local government and critical infrastructure networks, as well as for coordinating cyber incident response.
- 2 United States Department of Homeland Security, *Privacy Impact Assessment Update for the Private Sector Clearance Program for Critical Infrastructure* (Mar. 7, 2018), <https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-020%28b%29-pscp-march2018.pdf>.
- 3 *Id.*
- 4 Executive Office of the President of the United States, *The Comprehensive National Cybersecurity Initiative* (2009).
- 5 Josh Rogin, NSA Chief: Cybercrime constitutes the “greatest transfer of wealth in history”, *Foreign Policy* (Jul. 9, 2012, 6:54 PM), <https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/>.
- 6 Executive Office of the President of the United States, *The Comprehensive National Cybersecurity Initiative* (2009).
- 7 *Id.*
- 8 *Project 12 Report: Improving Protection of Privately Owned Critical Infrastructure Through Public-Private Partnerships*, Public Intelligence, <https://info.publicintelligence.net/NetworkInfrastructurePublicPrivate.pdf>.
- 9 *Id.*
- 10 *Id.*
- 11 Exec. Order No. 13549, 75 Fed. Reg. 51609 (Aug. 18, 2010).
- 12 Exec. Order No. 13691, 80 Fed. Reg. 9349 (Feb. 13, 2015), <https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari>.
- 13 Department of Homeland Security, *Support to Critical Infrastructure at Greatest Risk (“Section 9 Report”)* Summary (May 8, 2018), <https://www.dhs.gov/publication/support-critical-infrastructure-greatest-risk-section-9-report-summary>.
- 14 CISA, *National Critical Functions*, Department of Homeland Security, <https://www.dhs.gov/cisa/national-critical-functions>.



**“THE CREATION OF CISA AND LAUNCH
OF THE NATIONAL CRITICAL FUNCTION
INITIATIVE PROVIDES AN EXCELLENT
OPPORTUNITY FOR A REVIEW [OF
CLEARANCE PROGRAMS] TO ... DRIVE
MEANINGFUL PROGRESS IN CRITICAL
INFRASTRUCTURE CYBERSECURITY”**



NSI

THE NATIONAL SECURITY INSTITUTE
At George Mason University's Antonin Scalia Law School

THE NATIONAL SECURITY INSTITUTE

Antonin Scalia Law School | George Mason University
3301 Fairfax Dr. Arlington, VA 22201 | 703-993-5620

[NATIONALSECURITY.GMU.EDU](https://nationalecurity.gmu.edu)

