HOMELAND SECURITY ADVISORY COUNCIL

Final Report: Information and Communications Technology Risk Reduction Subcommittee

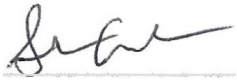
NOVEMBER 2020

Homeland Security

This page is intentionally left blank.

On behalf of the Homeland Security Advisory Council, Information and Communications Risk Reduction Subcommittee, Robert Rose, Chair, and Steve Adegbite, Vice Chair, present this final report and recommendations to the Acting Secretary of the Department of Homeland Security, Chad Wolf.

<SIGNATURE OBTAINED FOR PDF COPY>



Robert Rose (Chair)

Founder and President

Robert N. Rose Consulting LLC

Steve Adegbite (Vice Chair)

Former CSO, Cotiviti Corporation

This page is intentionally left blank.

Subcommittee on Information and Communications Technology Risk Reduction

Robert Rose (Chair)	Founder and President, Robert N. Rose Consulting LLC
Steve Adegbite (Vice Chair)	Former Chief Security Officer, Cotiviti Corporation
Keith Alexander	Founder and CEO, IronNet Cybersecurity
Jeff Moss	Founder of Black Hat and DEF CON Conferences
Paul Stockton	Managing Director, Sonecon LLC

Homeland Security Advisory Council Staff

Mike Miron	Acting Executive Director, Homeland Security Advisory Council
Evan Hughes	Associate Director, Homeland Security Advisory Council
Garret Conover	Director, Homeland Security Advisory Council
Colleen Silva	Analyst, Homeland Security Advisory Council

Additional Contributors

Anjana Rajan	Technology Policy Fellow, The Aspen Institute
Katharine Petrich	Research Fellow, Research on International Policy Implementation Lab, American University.
Amelia Mae Wolf	Truman National Security Fellow

This page is intentionally left blank.

TABLE OF CONTENTS

This page is intentionally left blank.

EXECUTIVE SUMMARY

The Department of Homeland Security (DHS) has significant and timely opportunities to reduce risks posed by the vital acquisition of information and communications technology (ICT). The Secretary of Homeland Security, the DHS team, and their private sector partners deserve credit for prioritizing improvements to supply chain security. The Homeland Security Advisory Council (HSAC) is honored to support these efforts through this report.

The HSAC's ICT Risk Reduction Subcommittee was asked to address four questions:

- What additional steps should DHS take to identify and mitigate its ICT supply chain risks?
- How effective are DHS's procurement efforts, and how might it increase the security of its ICT products?
- How might DHS better use its full suite of cybersecurity, law enforcement, trade, and customs authorities to identify and reduce ICT risks?
- In what areas might DHS better collaborate with the private sector to increase its shared understanding of supply chain vulnerabilities and threats?

Managing ICT risk is complex and difficult with many serious inherent challenges in accessibility, scope, and process. Actions by China and other nations pose increasingly grave threats to supply chains that provide the Department's ICT hardware, software, and support services. In addition, DHS must prioritize modernizing its own ICT systems to successfully execute its imperative missions, including countering cyberattacks launched from compromised ICT equipment. This report recommends five ways DHS can meet these challenges and produce a resilient, durable network to protect the country in the event of emergency or attack:

1. Develop an effective and robust risk management framework to guide ICT procurement across the government, with particular emphasis on unclassified systems;

2. Standardize the sharing and reception of threat data from the IC and across departments and agencies;

3. Establish a joint National Supply Chain Intelligence Center (NSCIC) Center of Excellence within DHS to operationalize and mature ICT risk reduction efforts;

4. Conduct a comprehensive review of the DHS procurement office authorities to ensure and maintain capabilities adequate for reducing ICT risks for the department;

5. Include and integrate the private sector into the effort to secure the ICT supply chain.

This page is intentionally left blank.

INTRODUCTION

What are Information and Communications Technologies?

Information and Communications Technology (ICT) is a broad term that includes all computer, software, networking, telecommuting, internet, programming, and information system technologies.[1] Due to rapid improvements in computer processing power, networking technology, programming interfaces, and the integration of ICT systems into organizational operations, such systems have become integral to our modern life.[2] Indeed, ICT systems go well beyond the computer networks and systems that are typically the focus of cybersecurity efforts and include operational systems[3] as well as so-called Internet-of-Things devices. ICT systems are pervasive throughout DHS, United States government, and the private sector and are essential to missions and everyday life.

ICT systems are critical to the federal government for many reasons beyond basic functionality. These systems allow governance to be more efficient, cost-effective, and responsive to citizen needs. They make the process of governing more accessible and transparent, which in turn increases public confidence in the government. ICT systems are particularly vital for large countries with significant rural areas, like the United States, because they help connect widely distributed communities with their representatives in government and provide access to information and services that, prior to ICT systems, would have been less available due to distance.

According to Cybersecurity and Infrastructure Security Agency (CISA), ICT systems are central to nine National Critical Functions (NCFs). The disruption of any of these NCFs would have catastrophic effects on national security, the economy, and global interconnectivity more broadly:

- The operation of core networks
- The provision of:
  - Cable access network services
  - Internet-based content, information, and communication services
  - Internet routing, access, and connection services
  - Positioning, navigation, and timing services
  - Radio broadcast access network services
  - Satellite access network services
  - Wireless access network services
  - Wireline access network services[4]

[1] "Information Communication Technology," University of Kentucky School of Information Science, accessed October 11, 2020, https://ci.uky.edu/sis/ict.
[2] "Information Communication Technology."
[3] Often referred to as Industrial Control Systems (ICS) or Operational Technology (OT Systems. These are any computer systems with real-time deadlines such as the electric grid, aircraft, industrial machinery, etc.
[4] "National Critical Functions Set." Cybersecurity and Infrastructure Security Agency, April 2016. https://www.cisa.gov/sites/default/files/publications/national-critical-functions-set-508.pdf.; "Executive Order 13873 Response: Methodology for Assessing the Most Critical Information and Communications Technologies and

Previous Work on the ICT Supply Chain

The concept of supply chain risk analysis is not unique to DHS; many other departments and agencies within the government, as well as private sector companies, engage in similar assessments. This duplication of effort, however well intentioned, results in imperfect information sharing about known risks and adversarial intentions and a tendency to over-focus on responding to the latest intellectual property (IP) theft rather than identifying future targets. As a result, the federal government has a less-than-holistic risk picture. Additionally, there is an overwhelming tendency to retroactively protect what has already been stolen rather than identify what is at risk in the future and proactively defend those technologies. Synchronizing efforts across the government would both reduce cost and increase security.

Previous government action and reports have identified ICT-related threats and concerns, and this subcommittee endorses the following recommendations:

Executive Order on Securing the Information and Communications Technology and Services Supply Chain[5]

President Donald Trump signed Executive Order (EO) 13873 in May 2019, directing the federal government to develop regulations and procedures to identify, assess, and address ICT-related vulnerabilities, particularly those threatening critical infrastructure or the American digital economy. This EO directed DHS to produce an initial written assessment of existing ICT threats "designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction of foreign adversaries," as well as conduct ongoing assessments of ICT threats.[6] This report and the subsequent threat evaluation methodology was completed by CISA in April 2020.[7]

CISA recommends a two-step approach to assessing the criticality of various ICT elements to continued government operations and to maintaining the nine National Critical Functions.[8] The first step is to determine the criticality of each ICT element in the context of the IT or communications sector function it supports. This approach enables a risk assessor to distinguish among similar elements used in different sub-roles. For example, a risk assessor might identify and evaluate the difference in the criticality of routers used in core networks responsible for routing terabytes of data as opposed to routers used in home networks for personal use. Once distinguished, such elements could be ranked as "critical," "manageably critical," or "not critical." Compromise of critical

---

Services" (Washington, D.C.: Cybersecurity and Infrastructure Security Agency, April 2020), https://www.cisa.gov/sites/default/files/publications/eo-response-methodology-for-assessing-ict_v2_508.pdf.

[5] Donald Trump, "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," Executive Order No. 13873, FR 84 22689 (2019), https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

[6] Trump.

[7] "Executive Order 13873 Response: Methodology for Assessing the Most Critical Information and Communications Technologies and Services."

[8] "Executive Order 13873 Response: Methodology for Assessing the Most Critical Information and Communications Technologies and Services."

elements would create an unacceptable amount of national security risk. Their compromise could affect operations and the confidentiality, integrity, or availability of critical data or systems, and it would be most problematic in cases where the ability to effectively mitigate these risks is uncertain or unsatisfactory.[9]

The subcommittee finds that, given the ability of such an approach to help evaluate ICT risk, it should be more widely employed by ICT security professionals both inside and outside the federal government.

Information and Communications Technology Supply Chain Risk Management Task Force (ICT SCRM) Interim Report[10]:

The ICT SCRM Task Force is a collaborative endeavor between industry and government designed to investigate and recommend methods to manage ICT supply chain risks. Members include 37 information technology and communications organizations and 17 government departments and agencies.[11] Formed in 2018, the Task Force was created to provide informed advice to both government and private sector critical infrastructure owners and operators on how to assess and manage ICT supply chain risks. The Task Force demonstrates how DHS's collective defense approach to cybersecurity risk management can benefit both government stakeholders and private industry.[12] The Task Force concentrates on four overlapping lines of effort:

- Information sharing
- Threat evaluation
- Developing qualified bidder and manufacturer lists
- Incentivizing the purchase of ICT from original equipment manufacturers (OEM) and authorized resellers

In addition, the Task Force is involved in developing an inventory of supply chain risk management efforts within government and industry and could be a model for future public-private collaboration.

The ICT SCRM Task Force represents the most complete repository of ICT supply chain-related strategy and industry mapping within the federal government.[13] However, securing

[9] "Executive Order 13873 Response: Methodology for Assessing the Most Critical Information and Communications Technologies and Services."
[10] Bob Kolasky, Robert Mayer, and John Miller, "Information and Communication Technology Supply Chain Risk Management Task Force Interim Report" (Washington, D.C.: Information and Communication Technology Supply Chain Risk Management Task Force, September 2019), https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf.
[11] Kolasky, Mayer, and Miller.
[12] Kolasky, Mayer, and Miller.
[13] Bob Kolasky, Robert Mayer, and John Miller, "Information and Communication Technology Supply Chain Risk Management Task Force Interim Report" (Washington, D.C.: Information and Communication Technology Supply Chain Risk Management Task Force, September 2019), https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf.

supply chains, particularly in the area of ICT, is an ongoing, dynamic process that needs to be an ongoing priority. This subcommittee builds on the excellent work of the Task Force in this report.

Cyberspace Solarium Commission

In March 2020, the bipartisan Cyberspace Solarium Commission published a report arguing for increased Congressional action on cybersecurity, particularly as it relates to cyber deterrence to adversaries.[14] Among the Commission's recommendations was the emphasis on resilient systems, supply chains, and the broader economy. Our globalized economic environment is characterized by offshore manufacturing, electronic storage, and tech support, which creates clear vulnerabilities to adversaries, either because facilities are less secure abroad or located in countries with a competitive relationship with the United States. This externalization means that information or processes critical to the success of the American people and economy can be stopped, slowed, or interfered with in times of crisis, creating a distinct area of vulnerability. This is particularly true for ICT-related areas. This subcommittee recommends that the Solarium Commission measures related to addressing ICT supply chain threats included in Appendix D be implemented to reduce risk and increase resilience in the United States.

[14] King and Gallagher, "Cyberspace Solarium Commission Report."

Information and Communications Risk Reduction

How should DHS identify and mitigate its ICT supply chain risks?

DHS has important leadership roles through the providing of risk guidance via CISA to other departments, agencies, partners, and allies, as well as exercising its regulatory authority to enforce proper security standards across government and its own ICT procurements. Additionally, DHS has statutory responsibilities to maintain ICT functionality in the face of an attack. DHS's analysis of ICT risk must go beyond the impact adversaries could have on DHS's own infrastructure and comprehensively address the risk carried by the private sector entities central to the NCF's. Private sector enterprises are now carrying significant unknown operational risks as state adversaries increasingly seek to exploit their enterprises and obtain access to ICT (and other) supply chains at scale. This suite of threats extends far beyond the realm of IT-based cyber-attacks, and therefore ought to be defined more broadly to also include operational risk and supply chain risk.

According to Christopher Nissen, Director of Asymmetric Threat Response & Supply Chain Security at MITRE, the U.S. currently has no clear comprehensive deterrence strategy for the "New Asymmetrical Era" in which the nation finds itself. [15,16] The American response to supply chain threats to-date has been limited to reactionary measures and reprisal. Mr. Nissen believes that the government must instead adopt a comprehensive deterrence strategy to ensure that critical infrastructure is defended effectively. Deterrence is realized when adversaries understand that any significant attack would be of negligible harm to the United States and/or such an action would be costly to them; at the heart of this robustness is critical infrastructure protection. Since critical infrastructure is primarily owned by the private sector, a strong public-private partnership for addressing ICT risk is essential. Building that collaboration between the government and private sector will therefore improve our national resilience to ICT threats.

To build this national resilience, DHS and the private sector must evolve its view on risk to be more proactive and move beyond a compliance-based approach to one of "owning the problem". This is not unprecedented in that today government and non-government organizations alike recognize the need for defensive cyber-IT protection measures. This was not always so. Today, the majority of these organizations ignore their supply chain vulnerabilities; this will not always be so.

How effective and secure are DHS procurement procedures?

The Office of the Chief Procurement Officer is a critical function at DHS, responsible for over $23.9 billion in the mission-critical products and services via more than 74,000 procurement transactions each year.[17] Soraya Correa, Chief Procurement Officer at DHS, states that the

[15] Christopher Nissen, DHS MITRE Briefing, interview by HSAC Subcommittee on ICT, June 4, 2020.
[16] "*Deliver Uncompromised"*, August, 2019, available at https://www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-26AUG2019.pdf
[17] Soraya Correa, DHS Procurement Briefing, interview by HSAC Subcommittee on ICT, April 7, 2020.

office works closely with five management directorate lines of business to fulfill integrated priorities, which ultimately helps DHS conduct smarter and more strategic sourcing. This collaboration lowers barriers of entry for innovative, non-traditional contractors to compete for DHS business. The Office also trains 13,000 acquisition professionals over 350 annual courses and maintains standards and certifications.[18] It keeps DHS compliant with complex policies, legislation, and reporting requirements.

Unfortunately, the Office of the Chief Procurement Officer does not have sufficient authority to effectively secure all ICT products used by DHS. Correa makes it clear that while the supply chain procurement process for classified use is largely secure because it is intrinsically given robust security consideration, the same does not hold for unclassified technology.[19] On the classified side, it is easier to work with vendors given well-defined requirements, a consistent list of vendors, and a process by which vendors can be rejected relatively easily because the acquisitions rules favor the government's discretion.

The procurement challenges lie in ICT products for unclassified use where the scope of risk is less clearly defined. On the unclassified side, it is more difficult to identify potential risks, especially with new vendors continuously entering the market. This variability on unclassified ICT is particularly challenging because procurement officers cannot easily determine why a particular company may have been deemed ineligible. Moreover, if the assessment is based on intelligence sources and methods, the agency has a limited ability to communicate to its management, as well as to other agencies, partners, and allies, a reason for a given vendor's ineligibility. A mechanism to communicate across agencies without compromising the integrity of the intelligence provided and while keeping up the speed of procurement should be developed.[20]

[18] Correa.
[19] Correa.
[20] Correa.

Recommendations of the Final Report

This subcommittee's analysis focuses on unclassified ICT products and recommends that DHS reshape its procurement practices accordingly.

Recommendation 1: Develop an effective and robust risk management framework to guide ICT procurement across the government, with particular emphasis on unclassified systems.

As disruption of unclassified systems could potentially hinder the execution of the Department's critical missions at any time, DHS should focus supply chain security initiatives and procurement processes on developing stringent guidelines for unclassified systems. Creating a risk management framework for unclassified systems can be accomplished with the well-known risk equation which considers risk to be a function of threat, vulnerability, and consequence:

1. Assess the potential consequences of successful attacks on the Department's ability to execute its critical missions. Who are the key adversaries and what would these adversaries gain by disrupting unclassified ICT systems?
2. With the help of the intelligence community (IC), assess the vulnerabilities of those systems to supply chain corruption and understand how and where adversaries are conducting attacks against the procurement system and the technologies it obtains.
3. Work with the IC to identify specific threats of greatest significance to unclassified ICT supply chains and products.

Risk management for ICT systems should also include identifying the layers of vendors and subcontractor relationships, mapping the supply chain (parts, components, software, and entities), and developing customized risk rating and mitigation methodologies,[21] as well as red teaming exercises to assess how key ICT systems function under stress.

Knowledge sharing across governmental silos remains a challenge for DHS and other agencies. Therefore, consensus on risk tolerance and standards for the whole of the federal government, not just DHS, should be further developed. DHS should take the lead in building out a more widely applicable risk management framework. An easily understood, effective, and scalable risk management framework widely propagated through the government would provide all departments and agencies with a common language around ICT risk and establish consistency across the federal system. DHS can iterate and build upon similar risk management frameworks previously established by the National Risk Management Center (NRMC), Department of Energy (DOE), and Department of Defense (DOD).[22]

[21] "Securing the Bulk-Power System," Guidehouse Consulting, 2020, https://guidehouse.com/insights/energy/2020/bulk-power-executive-order.
[22] Jon M. Boyens et al., "Supply Chain Risk Management Practices for Federal Information Systems and Organizations" (National Institute of Standards and Technology, April 2015), https://doi.org/10.6028/NIST.SP.800-161; Helen Jackson and John Miller, "Internet of Things Security Acquisition Guidance: Information Technology Sector" (Washington, D.C.: Cybersecurity and Infrastructure Security Agency, 2020),

Recommendation 2: Standardize the sharing and reception of threat data from the IC and across departments and agencies.

For the risk framework described above to be effective, it must be used with real-world, actionable data to include both intelligence insights and business information. Research and expert interviews suggest that the current capabilities and authorities are adequate at present, but that they need increased focus, alignment, and centralization. Heather McMahon, DOD Senior Executive and former Director for Counterintelligence Operations and Critical and Technology Protection, indicates that the DHS Procurement Office needs a more robust flow of data on the potential vulnerabilities of products they may be seeking to purchase. In fact, DHS has no consistent way of knowing which vendors have been identified as compromised or under investigation by US intelligence agencies. Insights and conclusions gained from acquisition authorities in one department of the government regarding potential ICT risks and threats across the public and private ICT ecosystem must be shared with other departments.

An excellent best practices model that DHS should emulate is DOE's 2013 Supply Chain Risk Management (SCRM) Awareness program.[23] Of particular value are the lessons learned from the SCRM Awareness program and the initial implementation measures that DOE is taking with regard to the executive order on building power system SCRM.[24] In addition, DHS might look to Executive Order 13920 (2020), which directed DOE to secure the "bulk power system" against potential hostile actors.[25]

Finally, with support from the IC, DHS should clarify emerging threats to unclassified ICT products. This task does not have to fall entirely on the shoulders of the Department. Rather, DHS should leverage the capabilities of other agencies and departments such as the General Services Administration (GSA) schedule. Recommendation three below is also central to addressing this challenge.

Recommendation 3: Establish a joint National Supply Chain Intelligence Center (NSCIC) Center of Excellence within DHS to operationalize and mature ICT risk reduction efforts.

https://www.cisa.gov/sites/default/files/publications/20_0204_cisa_sed_internet_of_things_acquisition_guidance_final_508_0.pdf; "Information and Communication Technology Supply Chain Risk Management" (Washington, D.C.: Department of Energy, September 27, 2012), https://www.directives.doe.gov/justification-memoranda/jm-205.1B/@@images/file.

[23] Boyens et al., "Supply Chain Risk Management Practices for Federal Information Systems and Organizations."

[24] Trump.

[25] Donald Trump, "Securing the United States Bulk-Power System," Executive Order No. 13920, FR 85 26595 (2020), https://www.federalregister.gov/documents/2020/05/04/2020-09695/securing-the-united-states-bulk-power-system.

In October of 2020, the Cyberspace Solarium Commission proposed that the government establish a National Supply Chain Intelligence Center (NSCIC)[26] (i.e., a Center of Excellence) to protect national security and maintain the rapid innovation at the core of the American ICT industry. The House Armed Services Committee (HASC) Future of Defense Task Force recently made a similar recommendation.[27] The proposed NSCIC would be chartered to share relevant information about suppliers that pose a national security risk with key private sector partners, while allowing private industry to share knowledge of potential vulnerabilities in technology with government agencies. By cutting through private sector norms of corporate competitiveness and IC norms of intelligence control, the NSCIC would build trust between government and industry, as well as broaden government understanding of risks and technology trends.

In addition, the NSCIC would facilitate the sharing of intelligence information from government analysts with other agencies, ensuring that the information is actionable, communicated, and utilized. The proposed NSCIC would allow DHS to bridge the work of the IC, impact government agencies, and enable effective decision making.

DHS should take advantage of the opportunity to centralize the management and maturity of existing ICT risk reduction efforts. The CISA ICT Supply Chain Risk Management (SCRM) task force has received considerable attention, but its scope is exceptionally far-reaching and broad. Thus, progress in this area has slowed as a result of the number of topics it must address, particularly those that are structural, strategic, and policy based. The delay has created an unintentional gap in providing operational and tactical capabilities. Establishing the NSCIC would help accelerate the efforts launched by the task force.

COEs have been used in industry and federal government agencies to address similar problems that must be resolved in parallel. Functional COEs have also provided critical long-term focus in maturing efforts and tend to work well in centralizing all efforts, capabilities, and authorities into one body dedicated to moving the problem forward. This dedicated focus can better leverage DHS's current powers and capabilities to:

- Develop a framework for public-private collaboration to identify ICT risks
- Provide and facilitate analytical support for DHS ICT risk reduction effort
- Provide detailed mapping of authorities, capabilities, and initiatives used to reduce DHS ICT risk for comprehensive gap analysis and remediation
- Develop and facilitate a centralized risk assessment to enable an understanding of all ICT risk down to the component-level (i.e., CBP, TSA)
- Research, collect, and develop ICT risk reduction, best practices, and standards

[26] Senator Angus King and Congressman Mike Gallagher, "Building a Trusted Supply Chain, Cyberspace Solarium Commission White Paper #4, October 2020, pp. 19 and 23, https://drive.google.com/file/d/1efo96fPx5WkOxTiFFY1r5y3lFqdit00C/view

[27] "*Future of Defense Task Force Report 2020",* House Armed Services Committee, September 23, 2020, Available at: https://armedservices.house.gov/2020/9/future-of-defense-task-force-releases-final-report

An additional benefit of the NSCIC would be its ability to bypass existing administrative reporting structures. It could be placed anywhere within an organization if its authorities and mission were formal. This flexibility allows for DHS to quickly form and place the NSCIC in any organization that DHS deems feasible.

The Commission did not specify where the proposed NSCIC should be placed within the federal interagency although the HASC Task Force recommended the National Counterintelligence Security Center (NCSC) within the Office of the Director of National Intelligence (DNI). This structure with Joint authorities with DHS, FBI and DOD would provide a robust interagency construct. Given the roles, responsibilities, and authorities of DHS for strengthening critical infrastructure against all hazards, including supply chain corruption, and the unique capabilities and expertise of the IC on threats to the supply chain, this subcommittee recommends that DHS and the IC jointly establish the NSCIC and that it also be designated as a DHS COE. DHS is well-placed to leverage the proposed center to rationalize and coordinate the overall structure of SCRM intelligence sharing.

.

The United States may also need to develop a national strategy or industrial policy on technology risks. While there is debate that such policy may stifle innovation, the risks of not having such a policy also poses an existential security threat; a sustainable middle ground is imperative. DHS should help lead such an effort.

Recommendation 4: Conduct a comprehensive review of the DHS procurement office authorities to ensure and maintain capabilities adequate for reducing ICT risks for the department.

At this time, DHS procurement functions may not have the necessary authorities to effectively prevent and mitigate ICT risk. Based on interviews and discussions with internal and external subject matter experts, this sub-committee believes, however, that the procurement function is an essential component for material reduction of ICT risk.

The challenge of outlining specific authorities is complex and wide-ranging, and it is unclear what additional authorities would best address this vulnerability. DHS should therefore endeavor to assess gaps in the present procurement authorities that are related to ICT specifically. This review will reduce pressure on policymakers to grant authorities that are broader than necessary.

Recommendation 5: Improve public-private partnerships specifically focused on the ICT security effort.

DHS could better collaborate with the private sector through: real-time sharing of classified and unclassified actionable threat information; building mutual trust through actions and shared experience (e.g., per how the Enduring Security Framework addresses key issues of mutual concern between the government and industry); helping promote collective security models for companies in key supply chains; and incentivizing performance and accomplishments in

meeting and exceeding best practices when it comes to addressing ICT risk.[28]

The DHS ICT Supply Chain Risk Management (SCRM) Task Force and private-sector organizations like the Charter of Trust have begun to step forward and articulate both the potential contributions and the concerns of the private sector in collaborating toward enhanced integrity for the supply chain that is shared by public and private sectors alike.[29] While the public sector can provide some insight from the IC, the private sector sees the earliest indications and warnings of potential problems in the supply chain. Together, these pieces of knowledge can create a stronger ICT supply chain; today, they operate separately. The next chapters of progress on ICT SCRM require persistent collaboration to provide robust mechanisms for increasing the shared understanding of contributions made by the private sector, as well as government.[30][31]

The private sector offers DHS some best-in-class examples of how ICT supply chain risks can be managed. DHS could:

- Use the Cybersecurity Capability Maturity Model (C2M2) and the NIST Cyber Security Framework (NIST-CSF) to identify, evaluate, and mitigate overall cyber risk, including relevant aspects of ICT supply chain risk.[32]
- Identify and implement industry-focused and -led best practices for ICT supply chain risk management by establishing appropriate corporate governance on ICT supply chain risk management. For example, as one key element of broadening cyber risk in this model, it could assign responsibility for ICT supply chain risk to a specific lead corporate officer, thereby ensuring appropriate, consistent reporting of such risk.

As the Department explicitly tasked with bringing the private sector into a relationship with the government, DHS could establish strong intra- and inter-industry and public-private information sharing relationships on ICT supply chain threats and technical capabilities to ingest and use actionable threat intelligence in real-time to mitigate such threats. The Department could implement audit controls to manage full life-cycle ICT supply chain risks. It could also create a trusted supplier network, which would make the process of continuously evaluating and validating the reliability of supplier networks significantly easier. As a function

[28] "Cross Sector - Enduring Security Framework Working Group," Cybersecurity and Infrastructure Security Agency (CISA), October 21, 2020, https://www.cisa.gov/publication/cipac-cs-esf-agendas.
[29] For more information on Charter of Trust, see: https://www.charteroftrust.com/.
[30] Ariel Levite, "ICT Supply Chain Integrity: Principles for Governmental and Corporate Policies," Carnegie Endowment for International Peace, October 4, 2019, https://carnegieendowment.org/2019/10/04/ict-supply-chain-integrity-principles-for-governmental-and-corporate-policies-pub-79974.
[31] "Information and Communications Technology Supply Chain Risk Management Task Force: Interim Report," Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security, September 2019, https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf.
[32] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1" (Gaithersburg, MD: National Institute of Standards and Technology, April 16, 2018), https://doi.org/10.6028/NIST.CSWP.04162018; "Cybersecurity Capability Maturity Model (C2M2) Program," Department of Energy, accessed October 12, 2020, https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0.

of this effort, DHS could establish close relationships with these trusted vendors through appropriate strategic partnerships, investments, and acquisitions. Finally, DHS could employ cyber insurance to mitigate the impact of ICT supply chain risk, by buying down risk through lower premiums for more secure ICT supply chains.

While public-private partnerships are essential to successfully managing ICT risks, several barriers exist today between the government and private sector. The lack of core trusted partnerships is the first barrier. Ineffective sharing of valuable, actionable ICT supply chain-related threat intelligence between the private sector and the government is the second. Moreover, to the extent they do share information, the process is agonizingly slow. The government has a strong regulatory instinct, while industry has a compliance-focused mentality; neither approach is likely to be successful in such a rapidly evolving technology marketplace.

A better approach is to identify the right incentives on both sides and build to that, rather than plaintively requesting coordination. An additional challenge is the fundamental disconnect between industry and government on the real scope, scale, and nature of the threats facing the ICT supply chain industry and how these threats might be most effectively mitigated. Finally, as noted by the Cyberspace Solarium Commission, there is a lack of fundamental agreement— a social compact— between the public and private sectors when it comes to appropriate roles and responsibilities with respect to managing and effectively limiting cyber risk, including ICT supply chain-related risks.

Within this recommendation, we believe it is important for DHS to take the lead in establishing and demonstrating how public-private partnerships can share actionable information at speed and scale in both classified and unclassified formats. By modeling and guiding this process, similar agency-industry cooperative paradigms might be applied to the federal government at scale. DHS should consider how efforts such as those recommended by the Open Group Trusted Technology Forum (OTTF) and others might be leveraged to enhance public and private sector ICT supply chain security and how to move such efforts through the International Organization for Standardization/International Electrotechnical Commission process more rapidly and effectively.[33][34] The slow, labyrinthian process of government procurement also makes participation by small companies and emerging technology firms less likely, disincentivizing some of the most innovative American suppliers.

The government can address some of these supplier challenges by making the procurement process clearer and more accessible, including revising regulations into plain language. It can also incentivize establishing robust domestic or allied ICT supply chains for key critical infrastructure assets by using government purchasing power, taxes, and other government incentive programs to motivate purchases from such supply chains, as well as by restricting the acquisition or use of certain foreign suppliers, capabilities, or assets in key areas or industries (e.g., as recent EOs have done with respect to telecommunications gear and bulk power-related

[33] The International Organization for Standardization/International Electrotechnical Commission is an independent, non-governmental international organization that develops standards to ensure the quality, safety, and efficiency of ICT products, services, and systems

[34] "The Open Group Trusted Technology Forum," The Open Group Website, accessed October 12, 2020, https://www.opengroup.org/membership/forums/trusted-technology-forum/trusted.

assets.)

Concurrently, DHS should encourage robust adoption and implementation—in both appropriate government and private sector organizations—of the following existing ICT best practices:

- NIST SP-800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations
- ISO/IEC 27036: Information Security for Supplier Relationships (Four Parts)
- SAE International Standards ARP9113
- Supply Chain Risk Management Guidelines
- Open Trusted Technology Provider Standard (O-TTPS)
- Mitigating maliciously tainted and counterfeit products (ISO/IEC 20243)).

By doing so, DHS could reconcile and normalize these guidelines and approaches where feasible from an economics, resource, and capabilities perspective.[35]

Further, DHS should revitalize and significantly expand the Enhanced Security Framework (ESF) efforts that are chartered by DHS and co-chaired by DHS, Office of the Director of National Intelligence (ODNI), and DOD. By refocusing the ESF efforts on getting near-, mid-, and long-term wins and ensuring that the new 5G working group is able to produce smart, effective, and aggressive recommendations on this issue, industry will be able to rapidly respond to potential ICT threats in a way that is both efficient and cost-effective.[36]

Any meaningful public-private partnership also requires trust built around a reciprocal flow of information. Policymakers should therefore seek to enhance the sharing of both classified and unclassified information with industry by granting more security clearances to private sector entities in critical infrastructure sectors in the interest of improving collective cyber defense against national security threats. Such clearances ought to be provided to industry participants for the specific purpose of conducting national security-related private sector defense, including defense of ICT and other key supply chains and routinizing such sharing of actionable threat data (e.g., within 180 days), including signatures and behaviors, to a real-time, machine-to-machine system that will allow the effective mitigation of ICT supply chain threats.

This process could be accomplished, in part, by ensuring that the National Security Agency (NSA) is specifically tasked and given the authorities and resources to prioritize the collection and dissemination of threat intelligence at all levels of classification about threats posed by foreign actors to the ICT supply chain, including private industry actors. Such action would require permitting the rapid and lower level declassification of applicable threat intelligence on ICT supply chain threats where the impact on collection would be limited relative to the gain expected for ICT supply chain security. Such an effort would also be enhanced if any ICT supply chain-related threat and mitigation information could be disseminated to the private sector through an appropriate homeland or national security agency such as the NSCIC recommended above artificially restricting the flow of information to industry to a single stovepipe in the interests of operational security could defeat the purpose of such sharing if it

[35] Boyens et al., "Supply Chain Risk Management Practices for Federal Information Systems and Organizations."
[36] "Cross Sector - Enduring Security Framework Working Group."

results in more limited or less timely sharing of actionable threat information.

APPENDIX A: Subcommittee Tasking

Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

February 21, 2020

MEMORANDUM FOR: Judge William Webster
Chair
Homeland Security Advisory Council

FROM: Chad F. Wolf
Acting Secretary, Department of Homeland Security

SUBJECT: **Four New Homeland Security Advisory Council (HSAC) Taskings**

Pursuant to the February 24, 2020 meeting of the Homeland Security Advisory Council, I am requesting that you establish four new HSAC subcommittees to undertake reviews of critical homeland security issues. The new subcommittees will be: (1) Economic Security; (2) Information and Communications Technology Risk Reduction; (3) Building Youth-Focused Engagements; and (4) Biometrics. An explanation and proposed scope for each subcommittee is listed below in items A through D.

Recommendations are due to the full Council no later than 180 days from the date of each subcommittee's formation. I would like an update and provisional findings from each subcommittee or panel at our next public meeting, which we will hold in early May 2020.

Thank you for your work on these important matters, your service on the HSAC, and your dedication to securing our homeland.

B. Information and Communications Technology Risk Reduction Subcommittee

The Information and Communications Technology Risk Reduction Subcommittee will explore the evolving risk of Information and Communications Technology (ICT) hardware and service threats against the United States and identify additional opportunities to counter them with DHS resources and authorities. The subcommittee should review the reports of the Cyberspace Solarium Commission and the Federal Acquisition Security Council prior to its final report and recommendations. The Subcommittee's mandate will include, but not limited to, the following:

1. What additional steps should the Department take to identify and mitigate its ICT supply chain risks?

2. Evaluate the effectiveness of the Department's procurement efforts and how it can increase security of its ICT products.

3. Examine whether DHS can better use its full suite of cybersecurity, law enforcement, trade, and its customs authorities to identify and reduce ICT risks.

4. What areas can the Department better collaborate with the private sector to increase its shared understanding of supply chain vulnerabilities and threats?

APPENDIX B: Biographies of Subcommittee Members

Robert Rose (Chair)
Founder and President
Robert N. Rose Consulting, LLC

Bob Rose is a recognized expert providing strategic counseling to the U.S. government and companies strategic counseling on a full array of issues at the nexus of cybersecurity, technology, national security, and privacy. He currently serves as Executive Vice President of 1Kosmos and is a member of its Advisory Board and as Senior Adviser to the Chairman of Securonix and is a member of its Advisory Board. Additionally, Bob is a member of the U.S. Department of Homeland Security's Homeland Security Advisory Council. Current corporate and non-profit advisory board service include The Chertoff Group, the Homeland Security Experts Group (formerly the Aspen Institute Homeland Security Group), Cyber Florida, Opora Technologies, Plurilock Security Solutions, and Auburn University's, Center for Cyber and Homeland Security, Council of Executives

Bob previously served as a senior advisor to the Chairman of Bridgewater Associates, and was an Advisory Board member of the National Security Agency's (NSA) Cyber Awareness and Response Panel, the Department of State's International Security Advisory Board, the National Counterterrorism Center (NCTC) Director's Advisory Board, and the Director of National Intelligence's (DNI) Financial Sector Advisory Board. Bob has received numerous honors and awards, including: a presidential appointment to the J. William Fulbright Board of Foreign Scholarship, a fellowship with the Wexner Heritage Foundation, the recipient of the U.S. Secret Service's "Outstanding Dedication and Contributions" award and the Connecticut Yankee Council of the Boys Scout's Distinguished Citizen Award.

He holds an active TS/SCI security clearance and received bachelor's degree from Georgetown University School of Foreign Service and a master's degree from Harvard University Kennedy School of Government.

Steve Adegbite (Vice Chair)
Former Chief Security Officer
Cotiviti Corporation

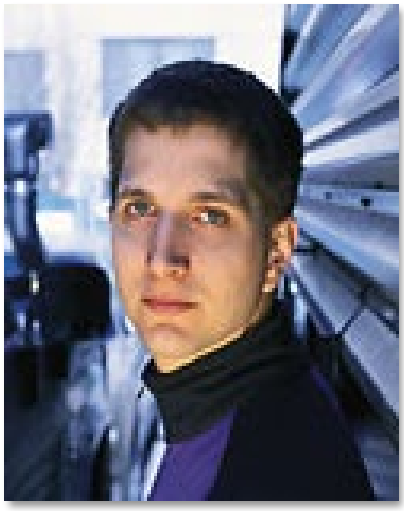
Steve Adegbite is the Former Chief Security Officer (CSO) at Cotiviti Corporation. He is the primary executive responsible for ensuring the establishing, executing, and maintaining of Cotiviti Corporation vision, strategy and program structure for all companywide security and business continuity programs. Prior to joining Cotiviti, Steve was the Chief Information Security Officer (CISO) for E*TRADE Financial Services. Prior to joining E*TRADE, he was the Senior Vice President in charge of the Enterprise Information Security Program Oversight and Strategy Organization at Wells Fargo & Co. Prior to joining Wells Fargo & Co., he was the Director, Cyber Security Strategies at Lockheed Martin Information Services and Global Services (IS&GS). Steve also severed as the Chief Security Strategist for Adobe Systems Inc. within the Adobe Secure Software Engineering. Prior to joining Adobe, he worked in various positions in Microsoft's Trust Worthy Computing (TWC) organization most notably on the Secure Windows Initiative (SWI) and Microsoft Security Response Center (MSRC) EcoStrat team. Before he joined the private sector, he was an officer in the United States Marine Corps and served in Information Operations (IO) positions at various Intelligence community agencies both as a government employee and as an associate consultant for Booz Allen Hamilton, a strategy and technology-consulting firm. Steve is longtime member of the US and International security community.

Keith Alexander
Founder & CEO
IronNet Cybersecurity

Keith Alexander is the CEO and President of IronNet Cybersecurity. In this position, he provides strategic vision to corporate leaders on cybersecurity issues through the development of cutting- edge technology, consulting, and education/training.

Alexander is a retired four-star General with a 40-year military career, which culminated to the role of Director of the National Security Agency (NSA) and Chief of the Central Security Service (CSS) from 2005-2014. He was appointed by Congress to be the first Commander to lead the U.S. Cyber Command (USCYBERCOM) from 2010-2014. As the Director of NSA, he was responsible for national foreign intelligence requirements, military combat support, and the protection of U.S. national security information systems.

Prior to leading USCYBERCOM and the NSA/CSS General Alexander served as the Deputy Chief of Staff, Intelligence, Department of the Army; Commanding General of the U.S. Army Intelligence and Security Command at Fort Belvoir, VA. He also served as: Director of Intelligence, United States Central Command, MacDill Air Force Base, FL.; Deputy Director for Requirements, Capabilities, Assessments and Doctrine, J-2, on the Joint Chiefs of Staff; and, a member of the President's Commission on Enhancing National Cybersecurity. General Alexander is the recipient of the 2016 United States Military Academy (USMA) Distinguished Graduate Award.



Jeff Moss
Founder of Black Hat and DEF CON Conferences

A career spent at the intersection of hacking, professional cybersecurity and Internet governance gives Jeff Moss a unique perspective on information security.

Mr. Moss is the founder and CEO of the DEF CON Communications and the founder of The Black Hat Briefings, two of the world's most influential information security conferences. Mr. Moss is an angel investor to startups in the security space, is a technical advisor to the TV Series Mr. Robot, and serves on the Board of Directors for Compagnie Financière Richemont SA.

Mr. Moss actively seeks out opportunities to help shape the cybersecurity conversation. In a prior life Mr. Moss served as the Chief Security Officer and was a Vice President of ICANN, the Internet Corporation for Assigned Names and Numbers. He is a member of the US Department of Homeland Security Advisory Council (HSAC) and a commissioner on the Global Council on the Stability of Cyberspace (GCSC). He is a Nonresident Senior Fellow at the Atlantic Council Cyber Statecraft Initiative, and a lifetime member of the Council on Foreign Relations.

Paul Stockton
Managing Director
Sonecon, LLC

Paul Stockton is the Managing Director of Sonecon LLC, and an internationally recognized leader in infrastructure resilience, continuity planning, installation and personnel security, and U.S. national security and foreign policy.

From June 2009 until January 2013, Dr. Stockton was Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs at the U.S. Department of Defense, where he served as the Department's Domestic Crisis Manager. In this position, he assisted in leading the response to Superstorm Sandy, Deepwater Horizon, and other disasters. In addition, he was responsible for Departmental programs strengthening security cooperation with partner nations in the Western Hemisphere, leading talks on Defense Cooperation Agreements with Peru, Brazil, and other key countries, as well as defense policy coordination with Mexico and Canada.

In September 2014, Secretary Hagel named Stockton the co-chair of the Independent Review of the Washington Navy Yard Shootings, which recommended major changes to the Department of Defense's security clearance system. He was twice awarded the Department of Defense Medal for Distinguished Public Service, the Pentagon's highest civilian honor, and a Distinguished Public Service Medal from the Department of Homeland Security.

APPENDIX C: Subject Matter Experts

1. James Burd, Acting Privacy Officer, Cybersecurity and Infrastructure Security Agency (CISA)
2. Soraya Correa, Chief Procurement Officer, DHS
3. Joyce Corell – Director of the Supply Chain Directorate, National Counterintelligence and Security Center (NCSC)
4. John Costello, Senior Director, Cyberspace Solarium Commission
5. Paul Courtney, Deputy Chief Procurement Officer, DHS
6. Frank Cilluffo, Commissioner, Cyberspace Solarium Commission; director Auburn
7. Pat Dowd, Director of Information Security, Amazon
8. David Frederick – Chief of Strategic Counter Cyber Operations, NSA
9. Chris Inglis, Commissioner, Cyberspace Solarium Commission, former Deputy Director, NSA
10. Jamil Jaffer, SVP for Strategy, Partnerships & Corporate Development at IronNet Cybersecurity
11. Sam Kaplan, Assistant Secretary for Cyber, Infrastructure, Risk and Resilience Policy, DHS
12. Bob Kolasky, Assistant Director, National Risk Management Center, Cybersecurity and Infrastructure Security Agency (CISA)
13. Bill LaPlante – Senior Vice President and General Manager, MITRE National Security Sector
14. Rick Ledgett, former Deputy Director, NSA
15. David Lindner, Senior Director, Privacy Policy and Oversight, DHS
16. Jeanette Manfra, Global Director, Security and Compliance, Google
17. Heather McMahon –Department of Defense Senior Executive and counterintelligence expert
18. Mark Montgomery, Executive Director, Cyberspace Solarium Commission
19. Chris Nissen, Director of Asymmetric Threat Response and Supply Chain Security, MITRE
20. Jaclyn Rubino, Executive Director, Strategic Programs Division, DHS
21. Ann Van Houten, Executive Director, Acquisition Policy and Oversight, DHS
22. Bryan Ware, Assistant Director, Cybersecurity, Cybersecurity and Infrastructure Security Agency (CISA)
23. Bill Zielinksi, Assistant Commissioner for the Office of Information Technology Category, GSA

APPENDIX D: Additional Recommendations

Cyberspace Solarium Commission

The ICT Risk Reduction subcommittee of the Department of Homeland Security Advisory Council (HSAC) has reviewed the Cyberspace Solarium Commission's Report and strongly endorses DHS's support of the Commission's recommendations 2.1.6., 3.1, 3.1.2, 3.3.1, 4, 5.1, and 5.1.2, as listed below.

- *Recommendation 2.1.6: Improve attribution analysis in conjunction with ODNI.*[37] Accurate and timely attribution of a cyber incident enables US leaders to make the most informed decisions to protect the country through consideration of appropriate response actions to enforce norms of accountability in cyberspace. The Office of Director of National Intelligence (ODNI), in partnership with the private sector through DHS and the FBI, should improve attribution analysis. This subcommittee joins the HSAC Economic Security Subcommittee in further endorsing this recommendation.

- *Recommendation 3.1: Increase Cybersecurity and Infrastructure Security Agency (CISA) authority to coordinate the sector-specific regulatory agencies.*[38] Critical infrastructure resilience and national risk management depend upon partnerships between the federal government and the private sector. These relationships are managed by sector-specific agencies; but their approaches are inconsistent, which gives rise to gaps in preparedness. Congress should increase CISA's supervisory authorities and recognize the Agency's lead role in managing national risk. This subcommittee joins the HSAC Economic Security Subcommittee in further endorsing this recommendation.

- *Recommendation 3.1.2: Create and resource a joint CISA-FEMA fund for resilience initiatives.*[39] While the Homeland Security Grant Program and resourcing for national preparedness under the Federal Management Agency (FEMA) are well-established, no equivalent funding stream exists for cybersecurity preparedness. Market forces do not provide sufficient private sector incentives to mitigate cyber risk, and a resilience grant system specifically targeted at cyber preparedness and attack prevention would significantly enhance the security and resilience of critical infrastructure. A joint program between CISA-FEMA would leverage area expertise (CISA) and administrative experience (FEMA), increasing the likelihood of success.

- *Recommendation 3.3.1: Designate DHS as lead agency for identifying cybersecurity services essential to national security.*[40] No single federal agency is currently tasked with this mission. By prioritizing and designating responsibility for continuity of cyber operations through executive order, the President should task DHS to identify: cybersecurity-related services essential to national security, the private sector's incident response capacity, and the

[37] King and Gallagher, "Cyberspace Solarium Commission Report."
[38] King and Gallagher.
[39] King and Gallagher.
[40] King and Gallagher.

critical infrastructure that must be protected or swiftly repaired in the event of an attack.

- *Recommendation 4.1.1: Set up and staff Critical Technology Security Centers to test critical infrastructure devices.*[41] The US government (USG) currently lacks trusted entities to perform cybersecurity evaluations and testing, resulting in uneven threat assessments of critical infrastructure. By funding three Critical Technology Security Centers, Congress would help remedy this gap. The Centers would serve as a national focal point for existing and new research into cybersecurity and help provide a more holistic picture of US cyber-preparedness. Helmed by DHS, these Centers should include personnel from the Department of Energy, Department of Commerce, Office of the Director of National Intelligence, and the Department of Defense.

- *Recommendation 5.1: Codify the concept of systemically important critical infrastructure and provide support while imposing obligations on the owners of that infrastructure.*[42] This Commission recommendation expands on Executive Order 13636, which called for special attention to such critical infrastructure. DHS, with its risk management capabilities, should continue to play a large role in the process of identifying systemically important infrastructure. The Economic Security subcommittee believes that the Cyberspace Solarium's recommendation implicitly corrects a flaw in the executive order that should be made explicit. The executive order arbitrarily exempts from its coverage some of the infrastructure at the heart of our economy — commercial and consumer information technology (IT). To the extent this exception ever made sense, its justification was lost in the 2020 pandemic, when the main thing that kept our economy from collapse was the use of commercial and consumer IT. Therefore, Congress and the President should extend the definition of critical infrastructure to cover IT and should task DHS with the identification and administration of systemically important IT infrastructure.

- *Recommendation 5.1.2: Coordinate with DHS to collect private sector input on intelligence priorities relating to cybersecurity.*[43] There is no formal process to solicit private sector input to inform US national intelligence priorities and collection efforts. For a variety of reasons laid out below, DHS is in a unique position to assist in dissemination and analysis of intelligence affecting the private sector. For those reasons, the subcommittee particularly endorses the Cyberspace Solarium Commission's recommendation that this effort be led by DHS, Congress should provide the authorities and resources DHS will need to play this role.

[41] King and Gallagher.
[42] King and Gallagher.
[43] King and Gallagher.

Homeland Security Advisory Council Economic Security Subcommittee

The ICT Risk Reduction subcommittee of the Department of Homeland Security Advisory Council (HSAC) has reviewed the Final Report of the Economic Security subcommittee (forthcoming November 2020) and fully endorses the recommendations as listed below:

- *Recommendation 3: The intelligence community and DHS should create a joint supply chain intelligence center with private sector entities as participants and customers. The center should provide practical guidance about suppliers that may pose a particular risk. The center should also have influence on intelligence collection priorities and provide feedback to improve the quality of supply chain intelligence.* While combining the economic security unit with the CFIUS and Team Telecom unit makes sense, more capacity is needed. Currently, the office focuses on economic security in the context of single transactions, usually with a 45-day deadline. Such decision making can produce focused and prompt resolutions, but it does not deal well with broader supply chain issues, such as competitors who have received state assistance, whether in the form of subsidies or cyberespionage support. CFIUS cases are enormously valuable in identifying a supply chain problem but they rarely provide a complete solution to the problem they have uncovered. To go beyond individual cases to more strategic assessments will require more resources, and perhaps substantially more resources.
  CISA also has a role in supply chain analysis, and has more resources dedicated to the issue than any other part of DHS. That said, for the department to manage its enterprise-wide activities and functionally coordinate within the interagency the Office of Strategy, Policy and Plans has an important function to play. The roles of CISA and the Office of Strategy, Policy and Plans could be harmonized and integrated. The Deputy Assistant Secretary for Economic Security could perform this function, serving as a bridge between Policy and CISA. For efficient coordination, however, the roles and responsibilities of CISA and the Office of Strategy, Policy and Plans need to be better defined.

- *Recommendation 4: The Secretary should define roles and missions and coordination responsibilities between CISA and the Office of Strategy, Policy and Plans for the tasks of mapping civilian supply chain and economic security risk.* No matter how responsibilities are divided, the task is essential. In the long run, the nation needs the capability to identify all supply chain threats to its economic security, to prioritize them, and to construct a strategy for remediating the threats. This is what the Defense Department's IndPol does for our industrial base, and the events of recent years have demonstrated that we can no longer leave our economic security to chance and the market. DHS is a necessary participant in any such effort.
  That said, comprehensively mapping supply chains that might impact national economic security is a daunting task. Further, a comprehensive but superficial analysis of many key supply chains will not be nearly as useful as an in-depth understanding of high-priority industries combined with risk-informed assessments and recommendations for mitigation. DHS would make more progress, more quickly in this mission by prioritizing its efforts, establishing the right methodologies and capabilities, and building interdepartmental and interagency cooperation.

Put another way, DHS should not try immediately to do for the entire civilian economy what the Defense Department's IndPol does for the defense industrial base. Defense has much more experience, capability and resources focused on a much narrower set of industries and supply chains. DHS needs to choose its shots, emulating in some respects the Air Force Office of Commercial and Economic Analysis, which performs case studies rather than comprehensive analyses and which has earned a strong reputation by doing those studies well, rather than by seeking broad authorities and the bureaucratic competition that can engender.

- *Recommendation 5a: DHS should formalize its role in supplying data and risk management analysis to the Commerce Department pursuant to EO 13873.* There are other ways for DHS to expand its economic security programs. It can build from the current work of CFIUS and Team Telecom. It often occurs that a CFIUS or Team Telecom matter exposes a vulnerability not previously understood. But these authorities only allow the government to say permit or veto a particular transaction. Often some broader study of the industry and of possible actions in connection with the industry is needed. It should be possible to engage in such studies as a first step to a broader economy-wide analysis. The same is true for referrals from the Commerce Department under EO 13873.[44]

- *Recommendation 5b: As one possible first step, DHS should conduct industry-wide analyses of supply chain risks and remedies based on referrals from agencies participating in individual cases for CFIUS, Team Telecom, and EO 13873, with the goal of assembling a coordinated package of additional measures that will bolster US economic security.* One observation is that a close relationship between CFIUS and Team Telecom unit and the economic security team would facilitate referrals from CFIUS to DHS for a broader examination of supply chain issues that go beyond approving or conditioning a particular acquisition.

- *Recommendation 5c: Another possible step for DHS's economic security unit is to receive referrals from the Federal Acquisition Security Council.* That Council will consider the risks of allowing companies to act as suppliers to federal government agencies. But in many cases, barring a company from federal procurements does not fully address the threat it may pose to the private but critical US infrastructure. It should be possible for the Council to seek a broader study of a particular industry or company than the Council itself is designed to perform.
  One finding is that it is imperative for the Secretary to develop management processes to ensure ways to address immediate and containable economic security issues without overextending the office. The Economic Security Council can help the Secretary in developing this guidance.

- *Recommendation 5d: The DHS economic security unit should accept nominations for economic security reviews from DHS components concerned about their critical components.* Coast Guard, CBP, and TSA all purchase big-ticket hardware from suppliers; they have an interest in the long-term viability and security of their suppliers - and in a

[44] "Executive Order 13873 Response: Methodology for Assessing the Most Critical Information and Communications Technologies and Services."

choice of secure bidders in the future. These components may choose to refer one or more of these suppliers to the economic security unit for a deeper dive into the conditions of competition in the field and the risk that insecure suppliers may supplant those on whom DHS relies.

Emerging Technologies Unmanned Aerial and Ground Based Systems Recommendations:

The ICT subcommittee of the Department of Homeland Security Advisory Council (HSAC) has reviewed the Final Report of the Emerging Technologies Unmanned Aerial and Ground Based Systems (2020), and fully endorses the recommendations provided in their report as listed below:

- *Recommendation 1: Promote legislation and policies which bring the development and production of UAS under American control, particularly those UAS intended for USG use.*[45]
- *Recommendation 2: Require USG UAS to be wholly manufactured within the United States and that all UAS are capable of being prevented from sending information back to the manufacturer.*[46]
- *Recommendation 3: Subsidize or support domestic UAS production to bring costs in line with DJI and Chinese manufactured UAS.*[47]
- *Recommendation 4: Maintain third party validation of any new or updated software, firmware, hardware, or ancillary UAS applications to ensure no data leakage occurs with these updates.*[48]
- *Recommendation 5: Use the authorities granted through the 2018 FAA Reauthorization to increase TSA staffing and UAS specific programs.*[49]
- *Recommendation 6: Partner with DOH to author national counter-UAS policy to harmonize competing efforts and ensure any use of force is both justified and proportionate, and to provide guidance to local, state, and tribal partners.*[50]
- *Recommendation 7: Coordinate with other governmental partners like the Department of the Interior, US Capitol Police and US Park Police to develop UAS-use policies in federal spaces, particularly near sensitive buildings and locations.*[51]

---

[45] Thad Allen, Cathy Lanier, and Robert Rose, "Final Report of the Emerging Technologies Subcommittee Unmanned Aircraft Systems" (Washington, D.C.: Homeland Security Advisory Council, February 24, 2020), https://www.dhs.gov/sites/default/files/publications/final_report_hsac_emerging_technologies_subcommittee_uas_508_compliance.pdf.
[46] Allen, Lanier, and Rose.
[47] Allen, Lanier, and Rose.
[48] Allen, Lanier, and Rose.
[49] Allen, Lanier, and Rose.
[50] Allen, Lanier, and Rose.
[51] Allen, Lanier, and Rose.

- *<u>Recommendation 8:</u> Develop and host a cross-agency UAS task force focused on emerging and over the horizon technological innovations in both UAS capabilities and counter-UAS capabilities. This task force should be explicitly responsible for monitoring new relevant technology.*[52]

- *<u>Recommendation 9:</u> Develop a national registration system for tracking and identifying UAS operations in real time, such as an automated individualized radio tag or signal.*[53]

- *<u>Recommendation 10</u>: Deeply resource detection and defeat mechanisms other than GPS and radio frequency communication links as these areas of vulnerability are quickly becoming obsolete.*[54]

- *<u>Recommendation 11:</u> Educate legislators about the fast evolution of UAS technology and advocate for legislative speed and flexibility in UAS response.*[55]

[52] Allen, Lanier, and Rose.
[53] Allen, Lanier, and Rose.
[54] Allen, Lanier, and Rose.
[55] Allen, Lanier, and Rose.

APPENDIX E: Library Repository

Additional Information on the Development of Information and Communications Technology Industrial Strategy Subcommittee
Additional Information on the Development of information and communications technology industrial strategy subcommittee.pdf

Briefing to the HSAC ICT Risk Reduction Subcommittee
Author: Soraya Correa, Chief Procurement Officer
Department of Homeland Security
Attachment B - HSAC Briefing Deck

Building a Trusted ICT Supply Chain - CSC White Paper #4
Cyberspace Solarium Commission
CSC - Supply Chain FINAL.pdf

Campaign Plan: Unmanned Aircraft System Information Security Risks
Department of Homeland Security
UAS Information Security Campaign Plan - approved Dec 2018.docx

Commercial Solutions Opening Pilot Program Guide
Author: Office of the Chief Procurement Officer
Department of Homeland Security
DHS commercial_solutions_opening_pilot_program_guide.pdf

Compiled Notes from Briefings Relating to a Supply Chain Intel Center
HSAC Compiled Notes - Supply Chain Intel Center.docx

Cybersecurity-Supply Chain Risk Management Legislation and Department of Homeland Security Special Procurement Authorities Challenges and Opportunities
C-SCRM Legislation and DHS Special Procurement Authorities

Cyberspace Solarium Commission - Executive Summary
CSC Executive Summary.pdf

Cyberspace Solarium Commission - Final Report
CSC Final Report.pdf

Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War
Author: Chris Nissen, John Gronager, Robert Metzger, Harvey Rishikof
Deliver Uncompromised MITRE Study 8AUG2018 copy.pdf

Deliver Uncompromised: Motivations, Progress, Forward Strategy

Author: Chris Nissen, Director, Asymmetric Threat Response & Supply Chain Security
The MITRE Corporation
4JUN2020 DHS ICT DU Brief.pptx

DHS - Homeland Security Advisory Council - Subcommittee on IT Risk Reduction
Author: Bill Zielinski, Assistant Commissioner, Office of Information Technology Category
U.S. General Services Administration
DHS Advisory Council Briefing 2020 April 16.pptx

DSB Task Force on Cyber Supply Chain
DSB Task Force on Cyber Supply Chain.pdf

Executive Order on Securing the Information and Communications Technology and Services Supply Chain
Executive Order on Securing the Information and Communications Technology and Services Supply Chain.pdf

Four New Homeland Security Advisory Council (HSAC) Taskings
Author: Chad F. Wolf, Acting Secretary
Department of Homeland Security
20-0345 Signed AS1 HSAC Memo 02.21.20 (3).pdf

High Level Thoughts on CIFIUS & FIRRMA Enhancements
Author: Chris Nissen
MITRE
CIFIUS FIRRMA Additional Considerations for FY21.docx

Homeland Security Advisory Council Information and Communications Technology Risk Reduction Subcommittee Members
Draft Membership List Information and Communications Technology Risk Reduction Subcommittee.docx

Kaspersky Lab, Inc. v. United States Department of Homeland Security
Kaspersky Lab Case.pdf

Memorandum of Agreement Between the U.S. International Development Finance Corporation and the U.S. Department of Defense
DOD-DFC-SIGN-MEMORANDUM-OF-AGREEMENT-ON-DEFENSE-PRODUCTION-ACT.pdf

MITRE ATT&CK: Design and Philosophy
Authors: Blake E. Strom, Andy Applebaum, Doug P. Miller, Kathryn C. Nickels, Adam G. Pennington, Cody B. Thomas
MITRE
ATTACK_Design_and_Philosophy_March_2020.pdf

National Counterintelligence Strategy of the United States of America: 2020-2022
National Counterintelligence and Security Center
20200205-National_CI_Strategy_2020_2022.pdf

Other Transactions for Research and Prototype Projects Guide
Author: Office of the Chief Procurement Officer
Department of Homeland Security
DHS Other Transactions for Research and Prototype Projects Guide July 2019.pdf

Policy Memorandum 119-08: Addressing Cybersecurity Vulnerabilities of Small Unmanned Aircraft Systems
Author: R.D. Alles
Department of Homeland Security
Policy Memorandum 119-08 Addressing Cybersecurity Vulnerabilities of Small Unmanned Aircraft Systems.pdf

Progress and Challenges in Modernizing DHS' IT Systems and Infrastructure
Author: Office of Inspector General
Department of Homeland Security
Progress and Challenges in Modernizing DHS' IT Systems and Infrastructure.pdf

Prohibition on Unauthorized Procurement of Small Unmanned Aircraft Systems
Author: Catherine Benavides, Acting Executive Director
Acquisition Policy & Legislation
Acquisition Alert 20-09 Prohibition on Unauthorized Procurement of sUAS.pdf

Recent Legislative, Executive, and Judicial Actions To Manage Supply Chain Risk
Recent U.S. Government Supply Chain Actions_final.docx

Recommendations to HSAC Economic Security Tasking Subcommittee
Author: Nazak Nikakhtar, Assistant Secretary, Industry & Analysis
Department of Commerce
2020-07-04 Recommendations to DHS.docx

Strategy to Reassert America as the World's Leader in Micro-Server Technology
Author: Global Technical Systems
Congress Reassert America as the World's leader in micro-server production (005).docx

Summary Recommendations from a Deliver Uncompromised Perspective on Strengthening our ICT Posture
Author: Chris Nissen
MITRE
Nissen High Level Recommendations for ICT Security.docx

Technology and Law Academy: Emerging Issues in Technology and Law Online Course Schedule

2020-06-29 - TLA-EITL Online Course Schedule.pdf

The DHS Privacy Office and CISA Office of Privacy
Authors: David Lindner, DHS Privacy Office, Sr. Director, Privacy Policy and Oversight;
James Burd, Acting CISA Privacy Officer
Department of Homeland Security
HSAC.PRIV Briefing.ppt

US Dependence on China for Medicines: National Health Security Implications
Author: Rosemary Gibson, Senior Advisor
The Hastings Center
Rosemary Gibson presentation.pdf