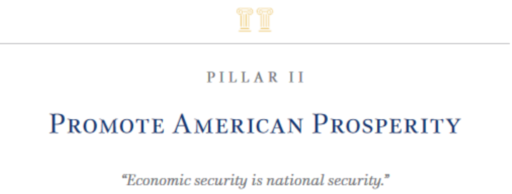
SUPPLY CHAIN RISK MANAGEMENT

CISA
CYBER+INFRASTRUCTURE

What Are We Talking About?

“Traditional” commercial SCRM perspective
vs.
Federal SCRM concerns

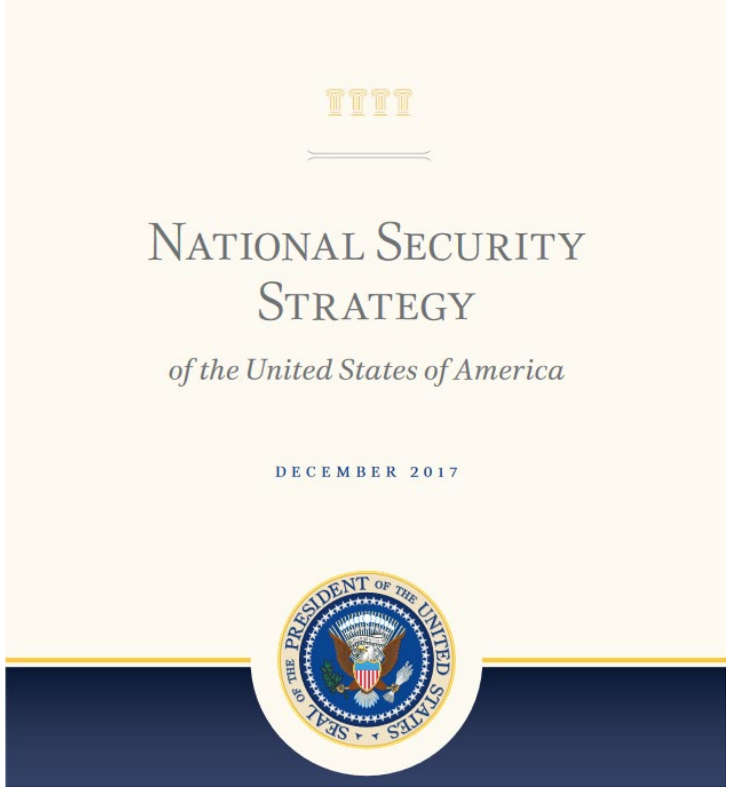


PILLAR II

PROMOTE AMERICAN PROSPERITY

“Economic security is national security.”

“[…] American prosperity and security are challenged by an economic competition playing out in a broader strategic context. The United States helped expand the liberal economic trading system to countries that did not share our values, in the hopes that these states would liberalize their economic and political practices and provide commensurate benefits to the United States. Experience shows that these countries distorted and undermined key economic institutions without undertaking significant reform of their economies or politics.”



NATIONAL SECURITY STRATEGY

of the United States of America

DECEMBER 2017

SCRM: Evolved

- A renewed focus on supply chain risk management (SCRM) in the context of national security, its importance to the prosperity of the larger U.S. economy, and its entwined cyber threats, make SCRM a new and critical aspect of CISA concern

- Increasing CISA is talking about SCRM as “National Industrial Base Security” to allow for a precise conversation both on the nature of the evolving threat and how CISA means to adapt to protect the U.S.

- SCRM has historically been seen as the purview of the Department of Defense under The Defense Production Act and derived from that laws Title 3 authority

- This historic lens has focused much of the discussion about supply chain security around those industries and applications that held intrinsic defense applications and largely ignored the greater uses to society.

SCRM: Evolved

Over the past 20 years globalization has created a sea change in the way business is conducted worldwide

The gradual but indisputable shift has exposed vulnerabilities and grey areas never before considered in the context of national security and the long term impact to the American people

Supply Chain Risk Management as a topic has been ill defined in addressing the ever growing importance it plays in national security

This catch all term has led to confusion about the specific nature of the associated risks and a lack of operational specificity about how to mitigate them

How We Talk Is How We Think

We need a better lexicon when it comes to talking about supply chain risk

- Activities should be segmented into mutually supporting but categorically distinct buckets through which the greater problem can be viewed and understood
- DHS needs to provide context in which security for industry can be discussed past the Defense Industrial Base, which is a narrow and specific facet of a much larger security issue.
- This subject in no way should be construed as a purely government problem with purely government solutions.

The goal is to *raise awareness* and open the narrative to encompass a whole of government and whole of nation approach to industrial base security

Framing supply chain security narratives in the context of industries that have equities that extend beyond, or have no association with, the Defense Industrial Base

SCRM and Cyber Security

3rd party risk is probably the greatest threat any company faces today when dealing with cyber security threats. Instances of sub-tier suppliers or ancillary vendors with poor cyber hygiene who inadvertently allow for the breach of a much larger company are well documented.

Hardware that is poorly designed and maintained represents a close second and is the most easily conceptualized threat for the average user. Instances of “island hopping” from a poorly secured device to another part of a larger network represent a significant number of cyber-attacks today.

Software assurance is another avenue of cyber supply chain risk that is gaining awareness and impact as companies begin to understand the impact poorly crafted software can have on their security posture.

The security of the products in this realm will define the future of innovation and are a clear and present national security risk to all industries – especially Critical Infrastructure

A Home Game and an Away Game

Threats to domestic national security are also directly impacted by concurrent tactics globally

Supply chain risk profiles must be continually assesses for evolving threats and prioritization of resources should flow to those areas where the impact would be unacceptably great

By engaging with Industry and partner nations around the world CISA is working to create mutually supporting systems that ensure American national security and prosperity in a globalized world.

Immediate Approach

Proactive Risk Identification and Mitigation

- In the same way that risk of a physical attack is evaluated in an effort to mitigate or avoid an incident prior to it occurring, risk to a supply chain – physical or digital – have to be approached the same way.
- Structures and methodologies have to be developed and put in place now to evaluate risk in a persistent and actionable way to arm both government leaders and industry with the information needed to act to mitigate them.

A Short Game and a Long Game

- Industry must act as both a clearing house and as an information source for risk as it exists presently and as it is identified.
- By leveraging the components across the USG and in particular the National Risk Management Center (NRMC) as the lead organization in risk threat identification related to domestic concerns, Industry and the USG can achieve the vital goal of addressing current risk while also forming a structure for future risk identification.

Evaluation at a Glance

While the risk of compromise is inherent in any technology that collects sensitive data or otherwise has access to critical systems, the risk increases considerably where the technology is produced or supplied by a company that could be persuaded or readily coerced to access that data or abuse that access on behalf of a foreign adversary

1. *The functionality and other vulnerabilities of the product*. What functions does the product or service perform and how does it operate? To what extent does the product operate with system or root level access on the network and systems on which it is installed? To what data does the product have access

2. *The country of origin of the supplier and its component suppliers*. What are the foreign government's national security interests as they relate to the United States? To what extent do the foreign government's laws or policies permit it to compel cooperation with its intelligence activities?

3. *The supplier's ties to the foreign government*. To what extent is the supplier owned, controlled, or otherwise influenced by the foreign government? Does the foreign government, whether directly or indirectly, hold a financial stake in the company?

SELECT USG ACTIVITIES

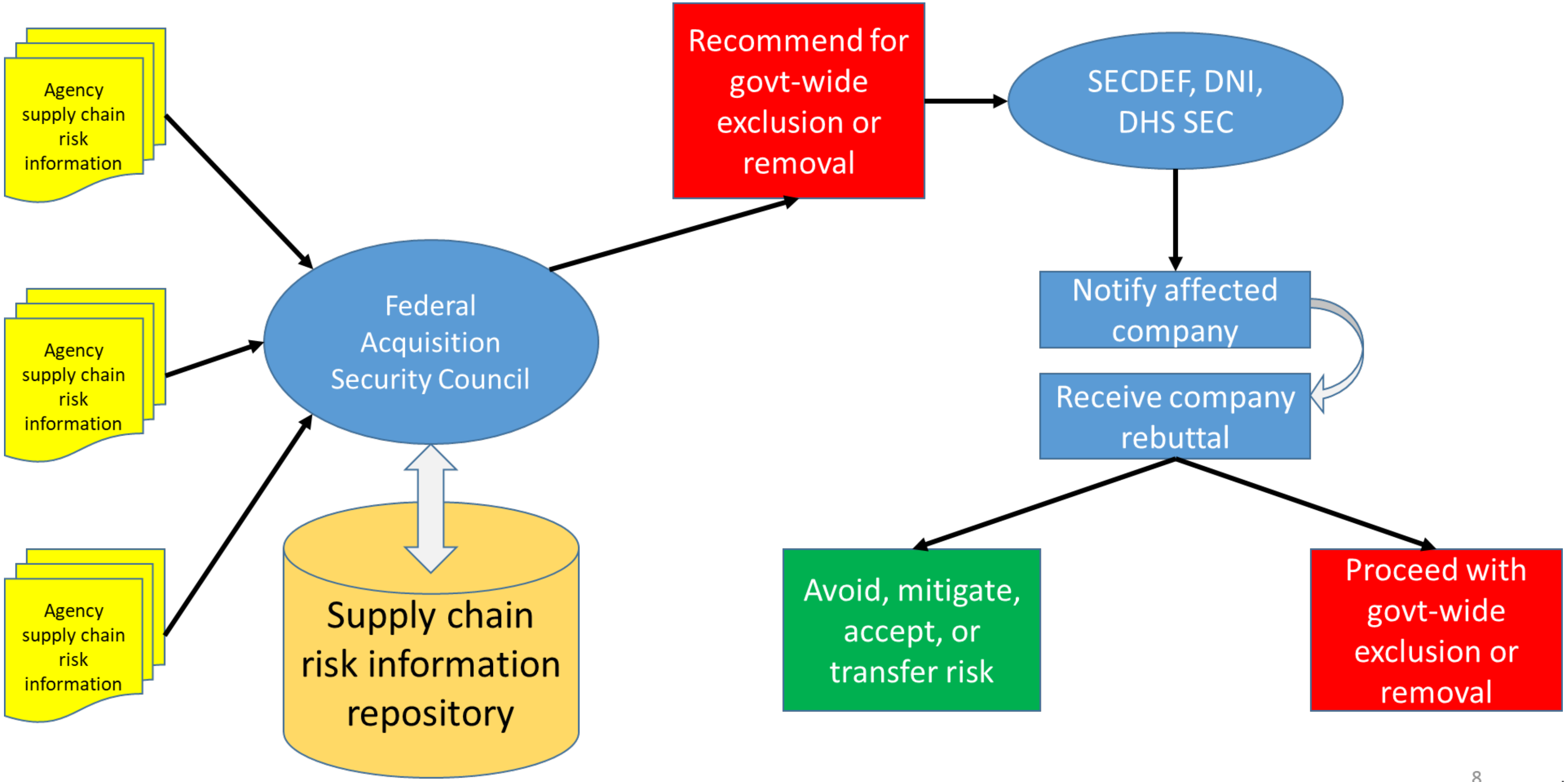
Federal Acquisition Supply Chain Security Act

The Federal Acquisition Supply Chain Security Act of 2018 (H.R. 7327, 41 USC Chap. 13 Subchap. III and Chap. 47, P.L. 115-390) (Dec. 21, 2018) has a significant effect on how the federal government buys and uses technology.

1. Requires all agencies to assess, avoid, mitigate, accept, or transfer supply chain risks. (41 USC 1326(a)(1))
2. Establishes the "*Federal Acquisition Security Council*" (41 USC 1322) to set supply chain risk management standards and manage government-wide supply chain risk management activities. (41 USC 1323-1328)
3. Vests the DHS Secretary* with authority to issue mandates for DHS and all civilian agencies to exclude sources (companies) from procurements and removal of "*covered articles*" (products and services) from information systems ("exclusion or removal orders"). (41 USC 1323(c)(5)(A)(i))
4. Vests the DHS Secretary with authority to assist executive agencies in conducting supply chain risk assessments, implementing mitigations, and providing additional guidance or tools as are necessary to support actions taken by executive agencies. (41 USC 1326(d))

*Authorities to exclude or remove are also vested in SECDEF for DoD systems and DNI for IC and NSS.

SCRM Process under FASCSA

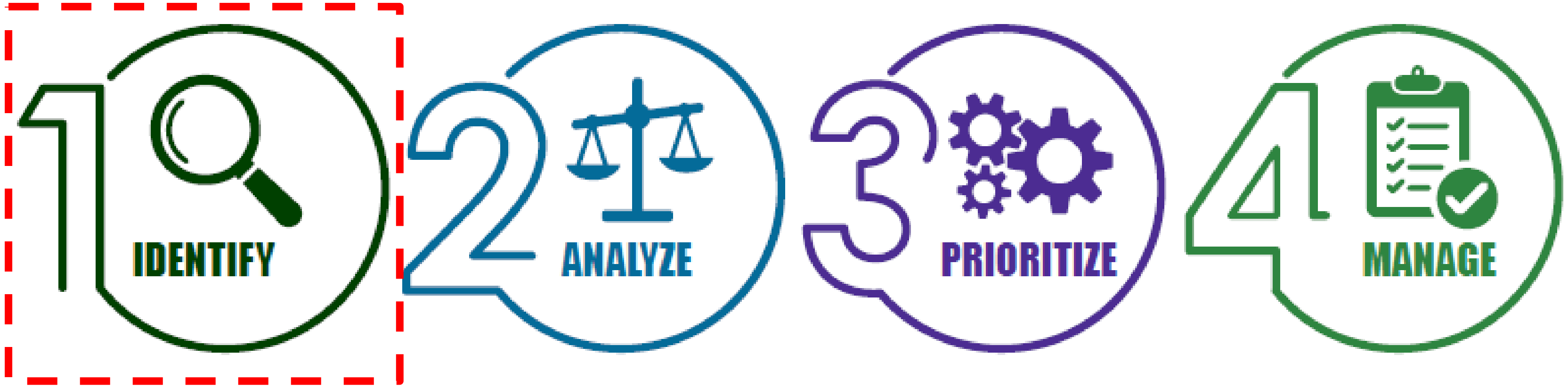

Agency supply chain risk information
Agency supply chain risk information
Agency supply chain risk information
Federal Acquisition Security Council
Supply chain risk information repository
Recommend for govt-wide exclusion or removal
SECDEF, DNI, DHS SEC
Notify affected company
Receive company rebuttal
Avoid, mitigate, accept, or transfer risk
Proceed with govt-wide exclusion or removal

8

Proposed process under review

National Critical Functions (NCF) – A Necessary Risk Management Evolution

“National Critical Functions” are the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.



COMPLETED

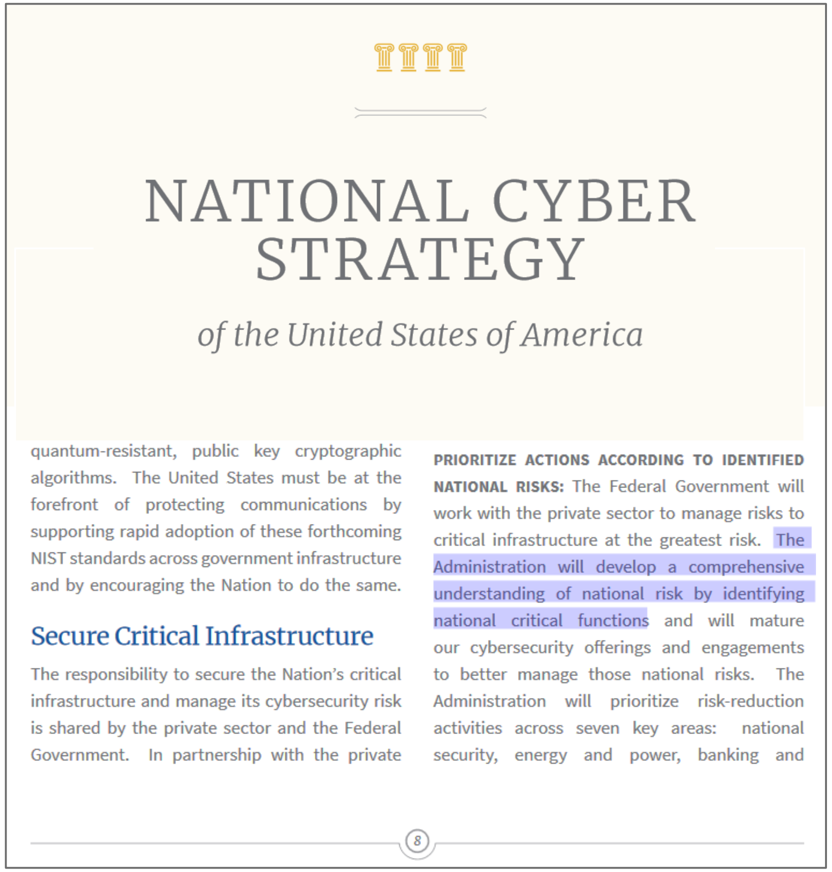
National Critical Functions

- It’s less about who you are. It’s more about the functions you produce or enable.
- Better captures cross-cutting risks and associated dependencies.

National Critical Functions set the stage for:

1. Supporting Infrastructure and Programmatic Prioritization
2. Conducting Detailed Operational and Risk Analysis
3. Informing Intelligence Collection Requirements
4. Supporting Incident Management Prioritization
5. Setting Priorities for Investments in Infrastructure Security and Resilience
6. Supporting National Security Decision Making
7. Enhancing the Efficacy of Continuity Efforts

The Mandate for National Critical Functions



NATIONAL CYBER STRATEGY

of the United States of America

quantum-resistant, public key cryptographic algorithms. The United States must be at the forefront of protecting communications by supporting rapid adoption of these forthcoming NIST standards across government infrastructure and by encouraging the Nation to do the same.

Secure Critical Infrastructure

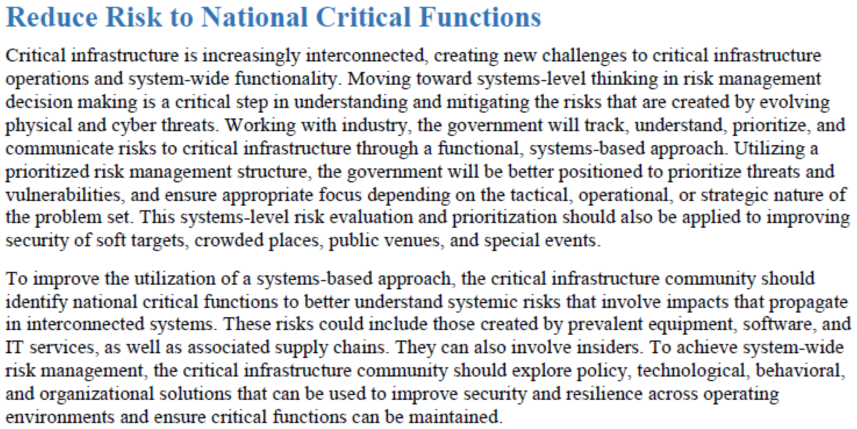
The responsibility to secure the Nation's critical infrastructure and manage its cybersecurity risk is shared by the private sector and the Federal Government. In partnership with the private

PRIORITIZE ACTIONS ACCORDING TO IDENTIFIED NATIONAL RISKS: The Federal Government will work with the private sector to manage risks to critical infrastructure at the greatest risk. The Administration will develop a comprehensive understanding of national risk by identifying national critical functions and will mature our cybersecurity offerings and engagements to better manage those national risks. The Administration will prioritize risk-reduction activities across seven key areas: national security, energy and power, banking and

8

2018 Joint National Priorities

Developed in Partnership with Critical Infrastructure Community



Reduce Risk to National Critical Functions

Critical infrastructure is increasingly interconnected, creating new challenges to critical infrastructure operations and system-wide functionality. Moving toward systems-level thinking in risk management decision making is a critical step in understanding and mitigating the risks that are created by evolving physical and cyber threats. Working with industry, the government will track, understand, prioritize, and communicate risks to critical infrastructure through a functional, systems-based approach. Utilizing a prioritized risk management structure, the government will be better positioned to prioritize threats and vulnerabilities, and ensure appropriate focus depending on the tactical, operational, or strategic nature of the problem set. This systems-level risk evaluation and prioritization should also be applied to improving security of soft targets, crowded places, public venues, and special events.

To improve the utilization of a systems-based approach, the critical infrastructure community should identify national critical functions to better understand systemic risks that involve impacts that propagate in interconnected systems. These risks could include those created by prevalent equipment, software, and IT services, as well as associated supply chains. They can also involve insiders. To achieve system-wide risk management, the critical infrastructure community should explore policy, technological, behavioral, and organizational solutions that can be used to improve security and resilience across operating environments and ensure critical functions can be maintained.

ICT TF

A supply chain is only as strong as its weakest link. The Department of Homeland Security's information and communications technology (ICT) supply chain risk management task force— the United States' preeminent public-private supply chain risk management partnership—was formed to identify and fortify any weak links that may exist in the ICT supply chain.

Work Streams

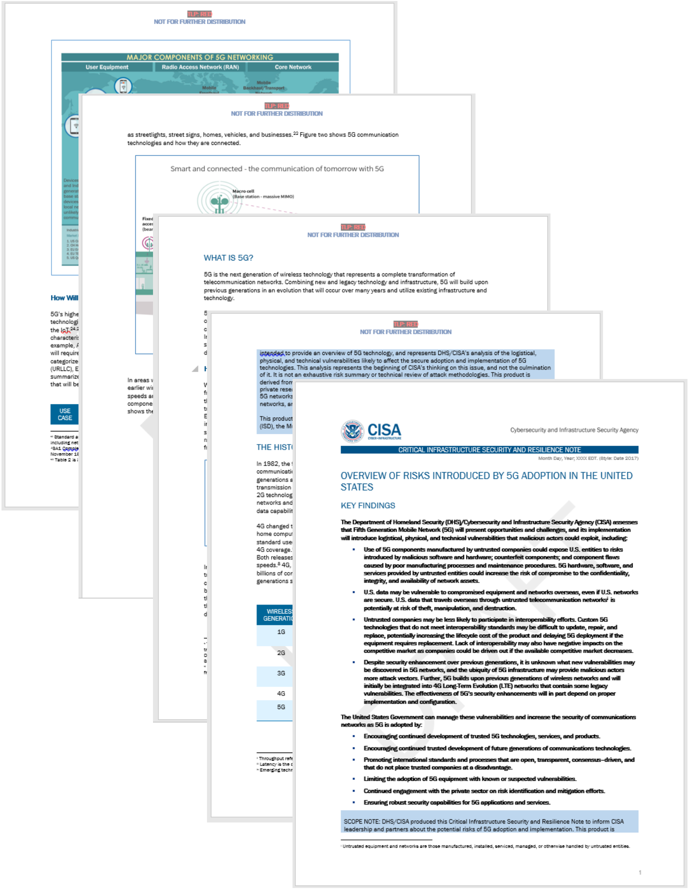
In addition to an ongoing inventory effort of existing public and private supply chain efforts, the Task Force is focusing its initial activity on the following work streams:

1. Developing a common framework for the bi-directional sharing of supply chain risk information between government and industry.
2. Identification of processes and criteria for threat-based evaluation of ICT supplies, products, and services.
3. Identification of market segment(s) and evaluation criteria for Qualified Bidder and Manufacturer List(s).
4. Producing policy recommendations to incentivize the purchase of ICT from original manufacturers or authorized resellers.

5G: Risk Characterization

5G Risk Characterization product provides a concise and easily understood overview of the wide range of risks 5G will introduce before, during, and after deployment

The document provides a foundational baseline that both USG and industry can reference as common ground during the deployment of 5G, and deeper analysis and work to mitigate known and future risk present itself



CISA

Cybersecurity and Infrastructure Security Agency

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE NOTE

Month Day, Year; XXXX EDT. (Style: Date 2017)

OVERVIEW OF RISKS INTRODUCED BY 5G ADOPTION IN THE UNITED STATES

KEY FINDINGS

The Department of Homeland Security (DHS)/Cybersecurity and Infrastructure Security Agency (CISA) assesses that Fifth Generation Mobile Network (5G) will present opportunities and challenges, and its implementation will introduce logistical, physical, and technical vulnerabilities that malicious actors could exploit, including:

- **Use of 5G components manufactured by untrusted companies could expose U.S. entities to risks introduced by malicious software and hardware; counterfeit components; and component flaws caused by poor manufacturing processes and maintenance procedures. 5G hardware, software, and services provided by untrusted entities could increase the risk of compromise to the confidentiality, integrity, and availability of network assets.**
- **U.S. data may be vulnerable to compromised equipment and networks overseas, even if U.S. networks are secure. U.S. data that travels overseas through untrusted telecommunication networks[i] is potentially at risk of theft, manipulation, and destruction.**
- **Untrusted companies may be less likely to participate in interoperability efforts. Custom 5G technologies that do not meet interoperability standards may be difficult to update, repair, and replace, potentially increasing the lifecycle cost of the product and delaying 5G deployment if the equipment requires replacement. Lack of interoperability may also have negative impacts on the competitive market as companies could be driven out if the available competitive market decreases.**
- **Despite security enhancement over previous generations, it is unknown what new vulnerabilities may be discovered in 5G networks, and the ubiquity of 5G infrastructure may provide malicious actors more attack vectors. Further, 5G builds upon previous generations of wireless networks and will initially be integrated into 4G Long-Term Evolution (LTE) networks that contain some legacy vulnerabilities. The effectiveness of 5G's security enhancements will in part depend on proper implementation and configuration.**

The United States Government can manage these vulnerabilities and increase the security of communications networks as 5G is adopted by:

- **Encouraging continued development of trusted 5G technologies, services, and products.**
- **Encouraging continued trusted development of future generations of communications technologies.**
- **Promoting international standards and processes that are open, transparent, consensus–driven, and that do not place trusted companies at a disadvantage.**
- **Limiting the adoption of 5G equipment with known or suspected vulnerabilities.**
- **Continued engagement with the private sector on risk identification and mitigation efforts.**
- **Ensuring robust security capabilities for 5G applications and services.**

SCOPE NOTE: DHS/CISA produced this Critical Infrastructure Security and Resilience Note to inform CISA leadership and partners about the potential risks of 5G adoption and implementation. This product is

[i] Untrusted equipment and networks are those manufactured, installed, serviced, managed, or otherwise handled by untrusted entities.

1

5G: Testing & Evaluation

Drawing on prior experience rapidly responding to emerging technological vulnerabilities by tapping our team at Idaho National Labs, which is conducting testing on voting equipment, to apply those lessons learned to 5G and improve the “out of the box” and implemented security of solutions/appliances/equipment

CISA intends to enumerate and exploit vulnerabilities with known or developed code/techniques, capture indicators of compromise information, capture exploitation methods to share with CISA assessment teams and develop mitigation strategies

5G: Broad Agency Announcement

The BAA establishes a “Security and Resilience of Mobile Network Infrastructure” Research and Development project within S&T’s Mobile Security R&D Program.

The BAA solicitation seeks proposals that address any or all three of the presented Technical Topic Areas:

1) 2G, 3G and 4G network protections.
2) Building security in to 5G networks and leveraging 5G to demonstrate solutions that meet government security requirements and also seeks end-to-end protection of network traffic, including a development of a standardized secure voice capability for unclassified government communications.
3) Innovative approaches to improve government visibility of network traffic from mobile devices to identify potential malware, attacks or attempts to exfiltrate data from or through the device.

U.S. DEPARTMENT OF HOMELAND SECURITY

CISA

CYBER+INFRASTRUCTURE