National Telecommunications and Information Administration

Plan to Congress on Declassification and Clearances related to The Communications Supply Chain Risk Information Partnership

November 2020

Background

The Communications Supply Chain Risk Information Partnership (C-SCRIP) was created in accordance with Section 8(a) of the Secure and Trusted Communications Networks Act of 2019 (Act). The Act tasks the National Telecommunications and Information Administration (NTIA) with facilitating the sharing of security risk information from the federal government to trusted providers of advanced telecommunications services and suppliers of communications equipment and services. The program aims to minimize the possibility that suppliers will include in their equipment and services—and that providers will embed in their networks—equipment or services that pose an unacceptable risk to U.S. national security or the security and safety of the U.S. population.

The Act requires NTIA to establish a program within 120 days to share information regarding supply chain security risks to trusted suppliers, with a focus on small and rural companies. Accordingly, NTIA announced the C-SCRIP program on July 8, 2020, describing a phased process to develop and implement the program.[1]

The Act also requires NTIA to submit this plan to Congress within 180 days for declassifying material, when feasible, and for expediting and expanding the provision of security clearances to facilitate information sharing. NTIA must ensure that the activities carried out through the program are consistent with and, to the extent practicable, integrated with ongoing activities of the Department of Homeland Security (DHS), including the Cybersecurity and Infrastructure Agency (CISA),[2] and the rest of the Department of Commerce, as well as the National Strategy to Secure 5G.[3]

NTIA sought broad input and feedback on this new program from interested stakeholders, including private industry, academia, civil society, and other security experts. The Request for Comments, required by the Act, was published on June 9, 2020,[4] and comments were published

---

[1] *See* NTIA, Notice: *Establishment of the Communications Supply Chain Risk Information Partnership*, 85 FR 41006, available at https://www ntia.doc.gov/federal-register-notice/2020/notice-establishment-communications-supply-chain-risk-information.

[2] In August 2020, CISA released its 5G Strategy detailing its approach to advance the development and deployment of a secure and resilient 5G infrastructure, one that promotes national security, data integrity, technological innovation, and economic opportunity for the United States and its allied partners. *See* DHS, CISA 5G Strategy, available at https://www.cisa.gov/sites/default/files/publications/cisa_5g_strategy_508.pdf. Additionally, CISA currently is developing its 5G strategic implementation plan, which will require a range of efforts from across the U.S. government and close collaboration with international and industry partners. CISA's 5G strategic implementation plan follows CISA's 5G Strategy and aligns with the National Strategy to Secure 5G and the Secure 5G and Beyond Act of 2020.

[3] *See* The National Strategy to Secure 5G of the United States of America, Mar. 2020, available at https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf.

[4] *See* NTIA, Request for Comments: *Promoting the Sharing of Supply Chain Security Risk Information Between Government and Communications Providers and Suppliers*, 85 FR 35919, available at https://www.ntia.doc.gov/files/ntia/publications/fr-rfc-promoting-sharing-supply-chain-security-risk-information.pdf.

on NTIA's web site on July 29, 2020.[5] The agency is considering these comments while designing a strategic implementation plan for the program. In addition to DHS, NTIA is coordinating heavily with government stakeholders, including the Office of Director of National Intelligence (ODNI), the Federal Bureau of Investigation (FBI), and the Federal Communications Commission (FCC).

Declassifying Material

The Act requires NTIA to report on its plan to declassify material, when feasible, to help share information regarding supply chain security risks with trusted providers of advanced communications service and trusted suppliers of communications equipment or services. To that end, NTIA and the C-SCRIP program will make the best use of existing government resources, analyzing available information and sharing such information at the appropriate level with trusted providers and suppliers.

NTIA does not originate classified material and does not declassify material. NTIA will achieve the C-SCRIP program's declassification requirements through formal relationships with members of the U.S. Intelligence Community (USIC), as well as the relevant civilian, military, and law enforcement agencies, working through existing programs at these other federal agencies.[6] Where required, NTIA will pursue specific memoranda of understanding with its interagency partners to meet C-SCRIP goals related to downgrading the classification level of intelligence products, tearlining (e.g., information cleared for disclosure or release) and security clearances. NTIA will work with the USIC on identifying supply chain risk information to share with the private sector.[7]

NTIA will also coordinate with existing programs already established at the Department of Commerce, including:

- Department of Commerce representative to the Federal Acquisition Security Council (FASC): NTIA will coordinate with FASC representatives on the sharing of relevant supply chain risk information. Like NTIA, the FASC has a responsibility to share supply chain information with the private sector. The FASC is responsible for sharing supply chain risk information across the federal government and with other non-federal entities. CISA serves as the Information Sharing Agency on behalf of the FASC.
- The Bureau of Industry and Security (BIS) Guardian Lead Program: Through this program, BIS shares information with companies to inform them of export-control-related issues of concern. NTIA is coordinating with BIS on best practices for industry outreach and process.

---

[5] *See* Comments on Promoting the Sharing of Supply Chain Security Risk Information, NTIA website, July 29, 2020, available at https://www ntia.doc.gov/federal-register-notice/2020/comments-promoting-sharing-supply-chain-security-risk-information-0.

[6] NTIA is a non-Title 50 (NT-50) federal agency and as such is not part of the Intelligence Community. NTIA does not hold the authority to produce and classify intelligence information, except through derivative classification.

[7] *See*, *e.g.*, Intelligence Community Directive 209: Tearline Production and Dissemination (Sept. 4, 2012), available at https://www.dni.gov/files/documents/ICD/ICD%20209%20Tearline%20Production%20and%20Dissemination.pdf.

- Office of the Secretary: NTIA will coordinate with the Office of the Secretary in implementation of Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain, to share any supply chain risk information identified, as appropriate, for sharing under the program.

Outside of the Department of Commerce, NTIA engages on information sharing issues with the following entities:

- DHS: CISA; the Communications and Information Technology Sector Coordinating Councils under the Critical Infrastructure Partnership Advisory Council (CIPAC); and the DHS Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force, of which NTIA is a member.[8] The C-SCRIP program will build on the ICT SCRM Task Force's work, particularly that of Working Group 1: Information Sharing. The ICT SCRM Working Group 1 report details the types of risk information that will be helpful to communications companies, which can inform intelligence gathering requirements. Although the report is not publicly available, additional information on the Task Force's information sharing efforts is available in the interim report.[9]
- ODNI: The Supply Chain and Cyber Directorate; and the new Supply Chain and Counterintelligence Risk Management Task Force, as called for in Section 6306 of the 2020 National Defense Authorization Act (NDAA).
- FBI: Science and Technology Branch; InfraGard; the Office of Private Sector; and the Office of the Chief Information Officer.

Expediting and Expanding the Provision of Security Clearances

The Act requires NTIA to report on its plan to expedite and expand the provision of security clearances to facilitate information sharing regarding supply chain security risks with trusted providers of advanced communications service and trusted suppliers of communications equipment or services.

As NTIA does not originate classified material, the agency intends to make use, to the maximum extent possible, of programs already in place to facilitate the provision of temporary security clearances for trusted providers of advanced communications service and trusted suppliers of communications equipment or services. NTIA has been working with DHS, ODNI, and the FBI to establish the parameters by which it can use the processes in place at those respective agencies that generated the classified information. Both DHS and ODNI have programs and authorities to provide temporary security clearances to private-sector representatives based on a clear set of established qualifications and guidelines. NTIA will use these programs to provide read-ins for specific briefings during the early phases of the program, but as the program and partnership

[8] *See* DHS CISA, Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force, available at https://www.cisa.gov/ict-scrm-task-force.

[9] *See* DHS CISA, Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM): Interim Report, Sept. 2019), available at https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf

matures, NTIA will determine the need to use other private-sector clearance programs. NTIA will seek to ensure that temporary read-ins and specific briefings are available at the state, regional, and local level to meet the needs of small and rural providers.

The Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities was established by Executive Order (E.O.) 13549 to ensure that security standards governing access to and safeguarding of classified information shared with private sector entities are applied uniformly, consistently, and in accordance with relevant previous orders.[10] Pursuant to E.O. 13549, the National Security Advisor provides overall policy guidance for the program. The Secretary of Homeland Security is designated as the Executive Agent (EA) for the program and implements and oversees its administration in consultation with the Director of the Office of Management and Budget, and the heads of affected agencies.

The program, known as the "Private Sector Clearance Program for Critical Infrastructure (PSCP)," is administered by DHS CISA and ensures that critical infrastructure private sector owners, operators, and industry representatives, specifically those in positions responsible for the protection, security, and resilience of their assets, are processed for the appropriate security clearances. NTIA will work with DHS CISA to use this program to share classified supply chain risk information with C-SCRIP partners.[11]

Should it become necessary in the future for NTIA itself to provide temporary access to classified information without the assistance of the agencies identified above, NTIA may use its authority through Security Executive Agent Directive 8.[12] SEAD 8 allows agency heads and designees to provide temporary access to classified information, temporary access to a higher level of classified information, one-time access to classified information, temporary eligibility to hold a sensitive position, and temporary eligibility to hold a higher-level sensitive position. If such actions are required, NTIA would notify and coordinate with the owners of the classified information that additional access was needed via their SEAD 8 authorities.

Implementing the C-SCRIP Program

NTIA is developing a strategic implementation plan for the C-SCRIP program to establish primary goals and operating principles for the partnership. The agency is using a phased approach to establish the program, in cooperation with its government partners.

In the current Phase 1, NTIA has established the program and developed this required report to Congress. NTIA issued an RFC and analyzed the submitted comments, which will inform the initial program plan. Also during this phase, NTIA has been coordinating closely with its federal partners to lay the groundwork to take advantage of the existing processes and procedures in place for the processing of security clearances and the declassification of threat intelligence.

---

[10] Exec. Order. No. 13549 75 Fed. Reg. 51609 (Aug. 18, 2010), available at https://www.federalregister.gov/documents/2010/08/23/2010-21016/classified-national-security-information-program-for-state-local-tribal-and-private-sector-entities.

[11] *See* DHS, Classified National Security Information Program for State, Local, Tribal and Private Sector Entities Implementing Directive (February 2012), available at https://www.dhs.gov/sites/default/files/publications/mgmt-classified-national-security-program-implementation-directive.pdf.

[12] Security Executive Agent Directive (SEAD) 8 (FOUO), V3.9, May 30, 2019.

In Phase 2, NTIA will establish the partnership community of providers and suppliers that are eligible under the Act to receive supply chain security risk information, and will begin to operationalize the program, including establishing partnership guidelines. NTIA will initiate briefings with trusted providers during Phase 2 on an ad hoc basis. NTIA will work with ODNI and other members of the Intelligence Community to ensure the community has actionable intelligence requirements that will be of use to the community of trusted suppliers and providers.

In Phase 3, NTIA will refine its methods and means for sharing information with the C-SCRIP partnership community to best secure U.S. communications networks against supply chain threats. NTIA also expects to formalize its process and schedule for briefings and alerts during this phase, and to establish formal mechanisms for ongoing coordination and communication.

During Phase 4, NTIA will evaluate the initiation period of the program and make recommendations for adjustments or enhancements to advance the goal of diminishing supply chain risk among program participants.

Conclusion

The United States believes it is critical to promote and invest in trusted vendors developing and building 5G components to avoid generational lock-ins that pose strategic national security and cybersecurity risks. Having a diversified network of trusted suppliers drives domestic economic opportunity and ingenuity now and into the future. It provides more options for securing our networks and better manages risk. It allows innovation to happen faster and in a modular fashion, and it allows additional security safeguards.

NTIA looks forward to engaging with Congress in the future as we build the C-SCRIP program.