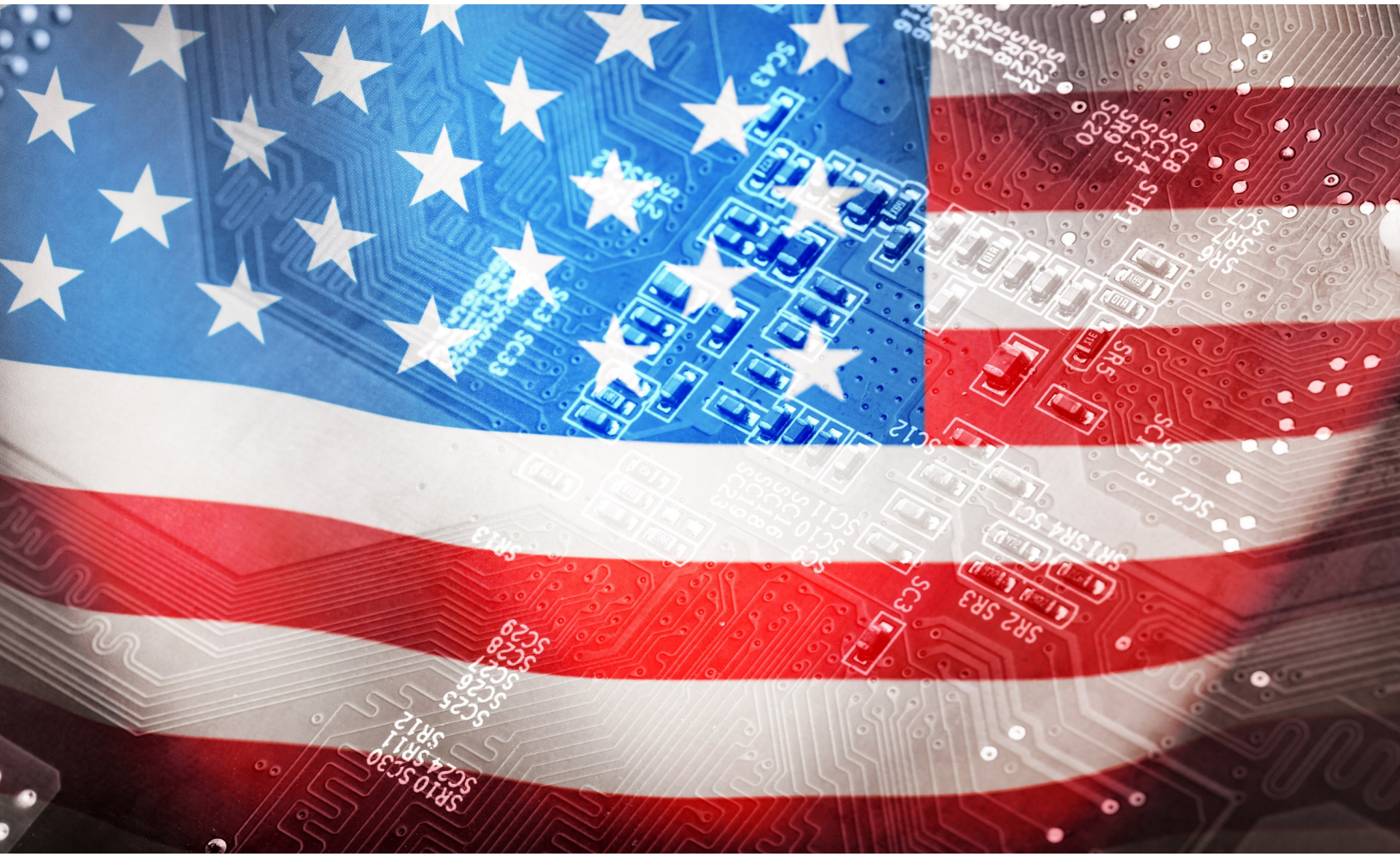
CHIPS Program Office

GUIDEBOOK

Approach to National Security

CHIPS Incentives Program

September 25, 2025



NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

CHIPS for America includes the CHIPS Program Office, responsible for semiconductor incentives and overseen by The Investment Accelerator within the Department of Commerce, and the CHIPS Research and Development Office, responsible for R&D programs. Both sit within the National Institute of Standards and Technology (NIST) at the Department of Commerce.

NIST promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. NIST is uniquely positioned to successfully administer the CHIPS for America program because of the bureau's strong relationships with U.S. industries, its deep understanding of the semiconductor ecosystem, and its reputation as fair and trusted.

Visit https://www.chips.gov to learn more.

This guidebook describes the CHIPS Program Office (CPO) approach to working with CHIPS applicants and awardees to advance national security.

The guide below is for informational purposes only. It does not, and is not intended to, supersede, modify, or otherwise alter applicable statutory or regulatory requirements, or the specific application requirements set forth in applicable notices of funding opportunities (NOFOs). In all cases, statutory and regulatory mandates, and the requirements set forth in NOFOs, shall prevail over any inconsistencies contained in the below guide.

Any reference to a non-federal organization or corporation does not convey endorsement or approval by the Department of Commerce of the entity or their programs or resources. All examples provided are for illustrative, non-exhaustive purposes only. The Department of Commerce does not guarantee the accuracy or completeness of the information contained therein.

Contents

1. Introduction

Semiconductors are integral to America's economic and national security, powering our consumer electronics, automobiles, data centers, critical infrastructure, and virtually all military systems. Today, however, many elements of the semiconductor ecosystem are geographically concentrated and produced outside of the U.S., leaving them vulnerable to disruption and endangering U.S. national security.

The Department of Commerce (DOC) is authorized by section 9902 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (CHIPS Act)[1] to provide:

> *"Federal financial assistance to covered entities to incentivize investment in facilities and equipment in the United States for the fabrication, assembly, testing, advanced packaging, production, or research and development of semiconductors, materials used to manufacture semiconductors, or semiconductor manufacturing equipment."*[2]

Pursuant to the CHIPS Act[3], the Secretary of Commerce will only approve CHIPS funding if it "is in the economic and national security interests of the United States." [4] To evaluate a project's potential contribution to U.S. national security, CPO evaluates an applicant's ability to:

- Reliably provide products usable by the military and critical infrastructure sectors;
- Secure sensitive information, equipment, and products; [5] and
- Manage supply chain security risks. [6, 7]

CPO also reviews projects for risks involving "foreign entities of concern" [8]and will not approve any applications where a foreign entity of concern — through control,[9] access to information, or other mechanisms — poses an undue risk to a project or to U.S. national security interests. Congressionally mandated guardrails prohibit any company that receives funding from engaging in significant transactions involving the material expansion of semiconductor manufacturing capacity in countries of concern for 10 years after the date of the award, subject to limited exceptions authorized in law.'[14] Further, the guardrails prohibit certain joint research and technology licensing initiatives that raise national security concerns.[15] These guardrails are intended to prevent recipients of CHIPS Incentives funds from enabling foreign countries of concern to gain access to technological advancements related to national security.

[1] Pub. L. No. 116-283, tit. XCIX, §§ 9902(2021) (codified at 15 U.S.C. §§ 4651 et seq.).
[2] 15 U.S.C. § 4652(a)(1).
[3] CHIPS Act of 2022, Pub. L. No. 117-167, Div. A (2022).
[4] 15 U.S.C. § 4652(a)(2)(C)(i)(II).
[5] For background information on relevant risks, see the following:
- The White House, *Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad- Based Growth*; 100-day-supply-chain-review-report.pdf.
- Defense Science Board, "Task Force on Cyber Supply Chain", (Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics, April 2017); semiconductor-supply-chain-2022-39E2C6B0-.pdf
- M. Rostami, F. Koushanfar, J. Rajendran and R. Karri, "Hardware security: Threat models and metrics," *2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, San Jose, CA, USA, 2013, pp. 819-823, doi: 10.1109/ICCAD.2013.6691207.

[6] The CHIPS Act specifies that applicants for CHIPS funding must have "an executable plan to identify and mitigate relevant semiconductor supply chain security risks, such as risks associated with access, availability, confidentiality, integrity, and a lack of geographic diversification in the covered entity's supply chain." 15 U.S.C. § 4652(a)(2)(C)(i)(III).
[7] With respect to projects for the production, assembly, or packaging of semiconductors, the CHIPS Act specifies that applicants must implement "policies and procedures to combat cloning, counterfeiting, and relabeling of semiconductors, as applicable."15 U.S.C. § 4652(a)(2)(C)(i)(IV).
[8] 15 U.S.C. § 4652(a)(2)(C)(v).
[9] The term "control" for this purpose is defined as any direct or indirect investment in a corporate entity that provides the investor with the means to influence important matters affecting the project. The term "means to influence important matters" includes membership or observer rights on, or the right to nominate an individual to a position on, the board of directors or equivalent governing body of the corporate entity; any involvement, other than through voting of shares, in substantive decision-making by the corporate entity; and consultation rights with respect to technology licensing to third parties.

CPO recognizes that it is impossible to eliminate all security risks or to have a perfect understanding of the risk environment. However, organizations can mitigate risks by adopting appropriate security protections. Organizations can also expand their ability to support critical infrastructure and military sectors by adopting procedures to handle classified, export controlled, and controlled unclassified information. High-level security practices are not required of all CHIPS funding recipients, but they represent an opportunity for organizations to meet the U.S. national security objectives of CPO.

2. Secure, Reliable Supply of Semiconductors

U.S. national security organizations and critical infrastructure sectors[10] require dependable access to reliable semiconductors, often with unique characteristics not typical in commercial applications.[11] These requirements may include specifications for raw material, size, reliability, security, quality, or performance. They may also include requirements for long lifespans that extend decades beyond their initial design. Today, sustaining such chips often requires the use of obsolete manufacturing equipment, obsolete processes, less secure designs, and rapid turn-around requirements, resulting in high costs to produce relatively low volumes of specialty semiconductors.

To strengthen U.S. national security, CPO seeks to fund projects that expand or modernize the production of chips that serve U.S. national security missions while also serving commercial markets. Such projects might produce chips that are used in weapons systems, data centers, communications and energy infrastructure, medical devices, or aerospace. These industries often also have unique specifications related to reliability, security, and performance that are not seen in the commercial market.[12] However, many projects that military and National Security industries are also likely to serve other commercial markets.

Projects that propose to serve only U.S. government customers will still need to demonstrate commercial viability and financial strength. In these instances, applicants can make a strong case that their project is critical to U.S. national security, demonstrate that alternative sources of U.S. government funding (e.g., from the DoD) are not available, or propose expanding into commercial markets. To illustrate their criticality to national security, applicants can identify what U.S. government programs and/or military contractors they support and to provide CPO with government points-of-contact who can validate the project's criticality to U.S. national security.

3. Applicant Approaches to Security

All semiconductor industry companies in the U.S., including those that produce entirely commercial products, face security risks that could impact National Security. The ability to proactively identify and quickly address security risks to semiconductor production is critical to U.S. national security. Consistent with applicable NOFOs, applicants will be required to demonstrate how they currently or plan to implement and enforce security practices in their organization and within the planned scope of the funded project.

[10] Presidential Policy Directive 21 (PPD-21)
[11] 100-day-supply-chain-review-report.pdf (whitehouse.gov) pages 26, 31.
[12] 100-day-supply-chain-review-report.pdf (whitehouse.gov) pages 26, 31.

3.1 Operational and Cybersecurity

Recipients of CHIPS funding should follow basic security practices to address risks such as:

- Financial and technical influence from foreign entities of concern;
- Espionage, sabotage, and insider threats;
- Cyber-related disruptions;
- Supply chain bottlenecks and dependencies;
- Obsolescence and supply shortages affecting the availability of needed parts or products;
- Tampering and hardware vulnerabilities;
- Theft of sensitive information and intellectual property; and
- Unreliable, poor quality, or non-genuine (counterfeit) products.

Projects that are capable of handling classified, controlled unclassified (CUI), and/or export-controlled information offer added benefits to national security because they create additional opportunities to increase production of chips that serve military and critical infrastructure sectors. Some industries have specific security requirements, such as Defense Federal Acquisition Regulation Supplement (DFARS) cybersecurity requirements, or aerospace industry standards. CPO expects that applicants will comply with any security-related obligations that are mandated by the specific customers or sectors they serve.

The Framework for Improving Critical Infrastructure Cybersecurity (CSF),[13] is a useful tool for applicants to evaluate and strengthen their approach to physical security, personnel security, supply chain risk management, and network security. The CSF can also help applicants communicate their security plans to CPO by mapping standards, laws, policies, and other company-specific documents to a common framework

3.2 Supply chain security and resilience

The semiconductor industry is a large, complex web of interconnected product and service providers. Supply chain partners and service providers are a target for foreign adversaries and criminals to compromise the confidentiality, integrity, availability, access, and resilience of semiconductor production and logistics. They are also vulnerable to the insertion of counterfeits, disruptions, and supply/materials shocks that may affect the availability of supply to the military and critical infrastructure sectors. Therefore, CHIPS incentive recipients should actively manage risks including:

- Ability to operate in the United States without access to non-U.S. facilities and personnel;
- Reliable access to utilities, transportation, and raw material inputs;
- The ability to acquire raw material, equipment, and components as needed even in the event of a major supply chain disruption, and
- The ability to identify foreign-owned or sourced inputs and mitigate associated risks.

To further strengthen supply chain security, recipients can adopt strategies to mitigate supply chain risks to the 4th and 5th tier of their supply chains. Strategies may include implementing incident response

[13] https://www.nist.gov/cyberframework.

and continuity of operations plans, conducting assessments and audits, performing stress test analyses, utilizing third-party continuous monitoring, and adopting supplier redundancy and agility policies.[31]

Applicants and recipients can provide as evidence to CPO relevant plans and policies, such as a supply chain risk management (SCRM) plan that addresses how the company identifies and mitigates risks originating from their suppliers and service providers. The plan could demonstrate how the project will address geographic concentration risks, will continue operating when faced with supply/materials shocks, and how suppliers and business partners are prioritized, evaluated, and monitored.

4. CPO Approaches to Mitigating Risks

The presence of security risks does not necessarily disqualify an applicant. CPO will evaluate applications based on their approaches to identifying and mitigating risks and will assess whether applicants' operational and SCRM practices are sufficient to protect against known threats. If an application is selected for funding, CPO may work with recipients to support companies' ability to:

- Implement security practices appropriate to the customers and industries they serve;
- Ensure that CPO investments do not benefit foreign countries of concern and foreign entities of concern; and
- Operate within the United States for a period of time without access to non-U.S. facilities and personnel.

Towards this aim, CPO's uses a security framework that defines the following broad categories for security:

- **Low:** For commercial projects that, if compromised, would likely have limited adverse effects on U.S. national security, minimum security and supply chain practices may be appropriate. These projects should still include a security and supply chain program that ensures the reliability of their products, the resilience of their supply chain, and the security of any sensitive information they handle (e.g., customer payment data).
- **Medium**: For projects that supply critical infrastructure to industries that, if compromised, would likely have a serious impact on national security,[37] enhanced security and supply chain practices may be appropriate. Security practices that ensure consistently high-quality products, prevent the production and use of non-genuine products, prevent foreign influence, and manage supply chain risks would be appropriate.
- **High**: For projects that support sensitive, national security-related sectors that, if compromised, would likely have severe or catastrophic effects on national security, strong security and supply chain practices are appropriate. These projects may include classified activities or production of critical, hard-to-obtain, or export-controlled products. In addition to meeting customer security and supply chain requirements (e.g., maintaining a classified environment), having a U.S.-based security program of sufficient size and maturity to mitigate sophisticated risks including tampering, insider threat, foreign influence in the supply chain, is expected.

Because each project will have a different risk posture and environment, the security practices they implement will be unique. CPO will work with applicants during the process on security mitigation approaches.

5. Conclusion

In implementing CHIPS Incentives funds, CPO's primary goal is to enhance U.S. economic and national security. This guidebook provides additional detail on how applicants and recipients can strengthen U.S. national security by producing a secure, reliable supply of semiconductors, especially for national security or military uses and critical infrastructure sectors; strengthening the operational security of proposed projects; and bolstering supply chain security and risk management practices. It also describes how CPO will evaluate applicant's contributions to national security and will work with funded projects to "raise the bar" on their security practices. In doing so, CPO aims to strengthen security practices across all funded projects and to create additional opportunities for projects to support military and critical infrastructure needs.

A. Glossary

The definitions listed below are intended to be informational and pulled from https://csrc.nist.gov/glossary unless otherwise noted.

- **Access Control** — The process of granting or denying specific requests to 1) obtain and use information and related information processing services and 2) enter specific physical facilities.

- **Contingency Planning** — Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters.

- **Continuous Monitoring** — Maintaining ongoing awareness to support organizational risk decisions. Note: The terms "continuous" and "ongoing" in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect an organization, its information, and its assets.

- **Critical Infrastructure** — System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

- **Cyber Insurance** — An insurance policy that provides entities with a coverage to help protect an entity from data breaches and other cyber security issues.

- **Cybersecurity** — The protection of data or information and the systems that process, transmit, or store that data or information. Cybersecurity typically involves managing risks to the confidentiality, integrity, and availability of data or information by preventing, detecting, and responding to malicious, unintentional, man-made, or natural threats to information and communication technology (ICT) or related systems. (Adapted from the Cybersecurity Framework Version 1.1 and NSPD-54/HSPD-23.)

- **Disaster Recovery Plans** — Written plans, management policy, and/or procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities.

- **Employee Training** — Teaching people the knowledge and skills that will enable them to perform their jobs more effectively.

- **Information and Communication Technologies (ICT)** — Devices or equipment involved in the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, or interchange of data and information. (Adapted from ISO/IEC 2382:2015.)

- **Network Segmentation** — An architectural approach that divides a network into multiple segments or subnets, each acting as its own small network allowing network administrators to control the flow of network traffic between subnets based on granular policies.

- **Redundant Capacity** — Additional capacity, bandwidth or other redundancies to limit the effects of information flooding denial-of-service attacks.

- **Sensitive Information / Sensitive Processes** — Data, information, or activities that are critical to the operations of the company or that, if compromised, could result in harm to national security. May include intellectual property, controlled unclassified information, and classified information. (Adapted from NIST SP 800-150.)

- **Supply Chain Risk Management (SCRM)** — A set of activities to assess and address risks associated with the distributed and interconnected nature of the logistics system(s) that produce and distribute products and services. (Adapted from NIST SP 800-161.)

- **Third Party Risks** — Any situations which might cause harm to the entity as a direct result of using another entity's products or services, generally through an agreement. In cybersecurity, this may be through the integration of another entity's vulnerable software code or the use of unverified service companies for maintenance support, for example. (Adapted from NIST SP 800-161 and 88 FR 37920.)