CHIPS for AMERICA

Approach to National Security

CHIPS Incentives Program

September 19, 2023

CHIPS for AMERICA

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 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.

1. Executive Summary

This guidebook describes the criteria that the CHIPS Program Office (CPO) uses to evaluate a CHIPS proposal's potential value to U.S. national security and CPO's approach to working with applicants to advance national security. It aims to serve as a reference for potential applicants as they consider what national security related information to include in their application.

The guide below is for informational purposes only and is intended solely to assist potential applicants in better understanding the CHIPS Incentives Program and the application requirements set forth in the February 28, 2023, Notice of Funding Opportunity (2023-NIST-CHIPS-CFF-01) *(CFF NOFO). The guide 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 the CFF NOFO. In all cases, statutory and regulatory mandates, and the requirements set forth in the CFF NOFO, shall prevail over any inconsistencies contained in the below guide. The Department will provide additional guidance regarding the applicability of this document to subsequent NOFOs.*

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

2. Introduction

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 may not approve an application for funding unless she determines "that the project to which the application relates is in the economic and national security interests of the United States."[4] 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."[5] With respect to projects for the production, assembly, or packaging of semiconductors, applicants must also implement "policies and procedures to combat cloning, counterfeiting, and relabeling of semiconductors, as applicable."[6]

In September 2022, DOC published *A Strategy for the CHIPS for America Fund* that sets overarching goals for the CHIPS Incentives Program, including providing financial assistance to produce secure and assured chips for national security uses. [7]

The CHIPS Program Office (CPO) subsequently released two "Vision for Success" documents, focused on commercial fabrication facilities and facilities for semiconductor materials and manufacturing equipment.[8,9] Through these Visions for Success documents, CPO articulated its investment objectives for strengthening U.S. economic and national security.[10]

[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] 15 U.S.C. § 4652(a)(2)(B)(iii).

[6] 15 U.S.C. § 4652(a)(2)(B)(iv).

[7] National Institute of Standards and Technology, United States Department of Commerce, *CHIPS For America Strategy*, 4 (CHIPS-for-America-Strategy (Sept 6, 2022).pdf).

[8] National Institute of Standards and Technology, United States Department of Commerce, *Vision for Success: Facilities for Semiconductor Materials and Manufacturing* (https://www.nist.gov/chips/vision-success-facilities-semiconductor-materials-and-manufacturing-equipment).

[9] National Institute of Standards and Technology, United States Department of Commerce, *Vision for Success: Commercial Fabrication Facilities* (https://www.nist.gov/chips/vision-success-commercial-fabrication-facilities).

[10] CPO's Vision for Success identifies the following goals: (1) Leading-Edge Logic: The United States will have at least two new large-scale clusters of leading-edge logic fabs, where clusters are geographically compact areas with multiple commercial-scale fabs owned and operated by one or more companies; a large, diverse, and skilled workforce; nearby suppliers; R&D facilities; utilities; and specialized infrastructure. (2) Advanced Packaging: The United States will be home to multiple high-volume advanced packaging facilities. (3) Leading-Edge Memory: U.S.-based fabs will produce high-volume leading-edge dynamic random-access memory (DRAM) chips on economically

This document builds upon these Visions for Success documents by providing additional detail on CPO's approach to U.S. national security, which includes an emphasis on increasing the production of semiconductors that support defense and other critical infrastructure sectors, as well as bolstering security practices across funded projects. This document is for informational purposes and can serve as a resource for potential applicants and their partners. It relates to the CFF NOFO but does not modify any requirements of existing or future funding opportunities or serve as a comprehensive security manual. The Department will provide additional guidance regarding the applicability of this document to subsequent NOFOs. We encourage applicants to include a national security section in applications that addresses applicable content in this guidebook.

3. Semiconductors and National Security

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 the global economy and U.S. national security. For example, many U.S. defense capabilities — including hypersonic weapons, drones, and satellites — are unduly vulnerable to supply chain disruptions. To strengthen U.S. national security, CPO aims to increase the domestic production of chips used by the U.S. defense industrial base.

Chip shortages have also affected critical infrastructure sectors, as evidenced by pandemic-related shortages in automobiles and medical devices. These shortages created negative economic effects and led to shortages of lifesaving equipment in American hospitals. To bolster U.S. national security, CPO also aims to increase the production of chips used by the critical infrastructure sectors defined by Presidential Policy Directive-21 (PPD-21), which includes telecommunications, critical manufacturing, power, automotive, and aerospace industries.

CPO will also boost U.S. national security by addressing security risks that affect the entire semiconductor ecosystem, including segments that serve the purely commercial market. These security risks include lack of access to or availability of semiconductors that meet security specifications, lack of integrity or quality control for semiconductor products and the production process, and compromises to the confidentiality of sensitive information. Specifically, CPO is focused on:[11]

competitive terms. (4) Current-Generation and Mature-Node Semiconductors: The United States will have increased its production capacity for the current-generation and mature-node chips most vital to U.S. economic and national security. Additionally, the CHIPS Program Office will invest to reduce chokepoint risks flowing from geographic concentration, advance U.S. technology leadership, and support vibrant U.S. fab clusters.

[11] For background information on these risks, see the following:

- 100-day-supply-chain-review-report.pdf (whitehouse.gov);
- Security Challenges and Requirements for Control Systems in the Semiconductor Manufacturing Sector (nist.gov);
- 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 (dni.gov)

- External influence from foreign entities of concern, including financial and technical influence;
- Espionage and insider threats, including intentional and unintentional sabotage or disruption;
- Cyber-related disruptions including ransomware, spyware, malware, or denial of service;
- Supply chain bottlenecks and dependencies, including as a result of geographic concentration;
- Obsolescence and supply shortages affecting the availability of needed parts or products;
- Tampering and hardware vulnerabilities, including misconfigurations, insertion of false data, and side-channel attacks;
- Theft of sensitive information and intellectual property; and
- Unreliable, poor quality, or non-genuine (counterfeit) products, including semiconductors, production equipment, sensors, and raw-materials.

CPO recognizes that it is impossible to eliminate all security risks or to have a perfect understanding of the risk environment. However, applicants can mitigate risks by adopting security protections related to foreign entities of concern, supply chain visibility and resilience, intellectual property protection, counterfeit mitigation, and cybersecurity. Applicants can also expand their ability to support critical infrastructure and defense sectors by adopting procedures to handle classified, export controlled, and controlled unclassified information. Such security practices are not required of CHIPS applicants. Instead, they represent an opportunity for applicants to meet the U.S. national security objectives articulated in the NOFO.

4. How The CHIPS Incentives Program Can Strengthen U.S. National Security

Advancing economic and national security is the principal objective of the CHIPS Incentives Program. To evaluate a project's potential contribution to U.S. national security, CPO will evaluate an applicant's ability to:

- Produce a secure, reliable supply of semiconductors, especially for the defense industrial base and critical infrastructure sectors;
- Maintain sufficient operational security of proposed projects; and
- Remain informed of and adopt best practices for supply chain security and risk management.

CPO will also review applications for involvement of "foreign entities of concern" [12] and will not approve any applications where a foreign entity of concern — through control,[13] access to information, or other mechanisms — poses an undue risk to a project or to U.S. national security interests. Additionally, CPO

- 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.

[12] 15 U.S.C. § 4652(a)(2)(C)(v).

[13] 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.

will implement congressionally mandated guardrails that 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. These guardrails will 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 will prohibit certain joint research and technology licensing initiatives that raise national security concerns.[15]

4.1 Secure, Reliable Supply of Semiconductors

The Department of Defense (DoD) and other national security organizations require dependable access to reliable semiconductors, often with unique characteristics not typical in commercial applications.[16] 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.[17] 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 projects that expand or modernize the production of chips that serve U.S. national security missions while also serving commercial markets. Consistent with the NOFO, CPO evaluates projects according to specific criteria, which include economic and national security, commercial viability, and financial strength. Projects that propose to support both national security missions and commercial markets are more likely to satisfy CPO objectives when evaluated against these criteria.

Example projects that support national security missions and commercial markets might include flexible, modular, secure, or standardized chip designs. CPO believes that projects of this type might open opportunities for the national security community to benefit from the innovation and economies of scale that are found in commercial markets. Such projects present an opportunity to reduce over time, the U.S. national security community’s reliance on low-volume, costly, and obsolete chips.

CPO is also aiming to increase the production of chips that serve the critical infrastructure sectors such as those defined by Presidential Policy Directive 21 (PPD-21). Such projects might produce chips that support data centers, communications and energy infrastructure, medical devices, and the automotive industry. These industries often also have unique specifications related to reliability, security, and performance that are not seen in the commercial market.[18] However, many projects that support PPD-21 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

[14] 15 U.S.C. § 4652(a)(6).

[15] *See, e.g.*, 15 U.S.C. § 4652(a)(5)(C).

[16] 100-day-supply-chain-review-report.pdf (whitehouse.gov) pages 26, 31.

[17] The White House, *Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth*, 56 (100-day-supply-chain-review-report.pdf).

[18] 100-day-supply-chain-review-report.pdf (whitehouse.gov) pages 26, 31.

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 defense contractors they support and to provide CPO with government points-of-contact who can validate the project's criticality to U.S. national security.

Importantly, according to some estimates, the semiconductor needs of the defense and critical infrastructure sectors represent less than 40% of the total market demand for chips.[19] Therefore, to increase U.S. national security, CPO is also aiming to increase the security, reliability, dependability, confidentiality, and integrity of all semiconductors, including those that serve purely commercial markets (e.g., are integrated into smartphones, PCs, cameras). Commercial "smart devices" can collect sensitive information, including users' personal information, and the chips they use can act as a gateway for accessing that information. The compromise of personal information can have public consequences and affect U.S. national security.

Therefore, applicants can describe how they will produce secure, reliable semiconductors by:

- Producing chips that meet unique national security requirements and also serve commercial markets;
- Obtaining advance purchase commitments from U.S. government agencies or known entities that support the defense industrial base and critical infrastructure sectors (e.g., defense contractors, major automotive manufacturers);
- Implementing policies and procedures to combat cloning, counterfeiting, and relabeling of semiconductor products (e.g., traceability programs); and
- Committing to continually improve semiconductor design and manufacturing process security to meet security requirements (e.g., by leveraging new approaches to combat counterfeiting, re-labeling, reverse-engineering, and hardware and firmware attacks such as code re-use, side-channel, fault-injection, digital trojans, induced degradation, and implement watermarking, environmental protections, and obfuscation).[20]

4.2 Operational Security

All applicants for CHIPS Incentives funds, including those that produce entirely commercial products, face security risks that may include attempts to disrupt or hamper production processes, such as through ransomware[21] and denial of service attacks and attempts to alter or steal sensitive or proprietary data,[22] including by insider threats. The ability to proactively identify and quickly address security risks to semiconductor production is critical to U.S. national security. These security risks may include:

[19] Analysis based on information from Gartner, TechInsights, and World Semiconductor Trade Statistics (WSTS).
[20] W. Hu, C. -H. Chang, A. Sengupta, S. Bhunia, R. Kastner and H. Li, "An Overview of Hardware Security and Trust: Threats, Countermeasures, and Design Tools," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 40, no. 6, pp. 1010-1038, June 2021, doi: 10.1109/TCAD.2020.3047976.
[21] Jonathan Greig, *Semiconductor industry faced 8 attacks from ransomware groups, extortion gangs in 2022,* The Record.
[22] 2012_IP_White_Paper_V2_SupAdd.pdf (semi.org).

- Intentional activities (e.g., espionage, tampering);
- Unintentional events (e.g., poor quality, negligence);
- Natural disasters (e.g., hurricane, earthquake);
- Internal sources (e.g., insider threat);
- External sources (e.g., utilities, third-party service providers, foreign criminals); and
- Unknown sources (e.g., outage or disruption with no known cause).

The semiconductor ecosystem is diverse and the specific risks that applicants face, along with their mitigation strategies, will be varied. For example, if an applicant proposes building a facility in a hurricane-prone area, they could construct a facility to resist category 5 hurricanes, plan to provide shelter for employees, have fail-safe and fail-secure mechanisms in case of flooding or loss of power, and purchase insurance that covers hurricanes.[23]

To strengthen U.S. national security, applicants should understand and follow basic operational security practices, including for the security of intellectual property, incident response and continuity of operations, counterfeit identification and mitigation, and other risks. Common best practices include access control, network segmentation, contingency planning, disaster recovery plans, redundant capacity, cyber insurance, employee training, and continuous monitoring.[24, 25] Applicants may also consider partnering with organizations dedicated to improving the semiconductor industry's overall security (e.g., by mentoring suppliers, participating in information sharing groups, or supporting standards development).[26]

Finally, some applicants may follow security requirements that are specific to the customers or industries they serve, such as Defense Federal Acquisition Regulation Supplement (DFARS) cybersecurity requirements, or automotive industry standards. CPO expects that applicants will comply with any security-related obligations that are mandated by the specific customers or sectors they serve. 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 defense and critical infrastructure sectors.[27]

4.3 Supply chain security and resilience

All applicants for CHIPS Incentives funds, including those that produce entirely commercial products, rely on large, complex, and interconnected networks of product and service providers. These third-party and supply chain partners are a target for foreign adversaries 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

[23] NIST SP 800-161, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, Appendix C: "Risk Exposure Framework", provides one way of examining and discussing threat scenarios. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf.
[24] CHIPS-Commercial_Fabrication_Facilities_NOFO_0.pdf (nist.gov).
[25] There are numerous guides and standards describing basic security practices, such as NIST IR 7621 (https://csrc.nist.gov/pubs/ir/7621/r1/final),or CISA security guides (https://www.cisa.gov/topics)
[26] National Institute of Standards and Technology, United States Department of Commerce, *CHIPS For America Strategy*, 16 (CHIPS-for-America-Strategy (Sept 6, 2022).pdf).
[27] CHIPS-Commercial_Fabrication_Facilities_NOFO_0.pdf (nist.gov) (page 59).

availability of supply to the defense and critical infrastructure sectors. Therefore, applicants can identify supply chain risks, which may include:[28]

- Physical Infrastructure: Access to power, water, air strips, and material transportation channels;
- Supplier Ecosystem: Raw material, equipment, and component supply chain acquisition strategies;
- Continuity of Operations: Ability to operate in the United States without access to non-U.S. facilities and personnel, consistent with applicable funding opportunities; and
- Transparency and Traceability: Understanding, visibility, and control of the supply chain and the ability to identify and mitigate risks associated with dependence on foreign-owned or sourced inputs, which create the potential that foreign entities of concern might access sensitive information, control activities, or otherwise pose undue risk to the project or U.S. national security interests.[29,30]

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

5. How the CHIPS Incentives Program Will Mitigate Security Risks

Each project funded through the CHIPS Incentives Program presents opportunities to strengthen U.S. national security; however, projects may also contain security risks. CPO will take a flexible and individualized approach to understanding and evaluating security risks during the application process. Applicants can both self-identify security risks and demonstrate a willingness to strengthen their own security practices. If projects are selected for funding, consistent with requirements in applicable notice of funding opportunities, CPO may work with awardees to strengthen their security practices to ensure that appropriate security standards are being met and to expand their ability to support defense or critical infrastructure sectors.

5.1 Applicant Approaches to Security

Consistent with the CFF NOFO, applicants should demonstrate how they currently or plan to implement and enforce security practices in their organization and within the planned scope of the funded project. The Framework for Improving Critical Infrastructure Cybersecurity (CSF),[32] 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

[28] CHIPS-Commercial_Fabrication_Facilities_NOFO_0.pdf (nist.gov).

[29] 15 U.S.C. § 4652(a)(2)(D)(i)(II).

[30] National Institute of Standards and Technology, United States Department of Commerce, *CHIPS For America Strategy*, 16 (CHIPS-for-America-Strategy (Sept 6, 2022).pdf).

[31] CHIPS-Commercial_Fabrication_Facilities_NOFO_0.pdf (nist.gov).

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

framework. Applicants may identify any security-relevant laws, regulations, rules, standards, guidelines, or other documents that are applicable to the industries or customers they serve, their physical location, and the type of information or data they handle. Applicants can also review the most recent version of NIST Special Publication 800-53,[33] which contains a large catalogue of security measures organizations may use, with baseline recommendations at low-impact, moderate-impact, and high-impact risk levels. Additional guidance can be found in NIST Special Publication 800-, 500-, and 1500- series of documents, as well as publications from the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).[34]

Applicants may consider providing evidence of their security practices to reduce the amount of time and effort it will take to verify the information provided. For example, if an applicant claims that they are certified to ISO 9001, they can provide CPO with their certificate information. If an applicant claims to be compliant with NIST SP 800-171 and provide products to DoD, they can provide CPO with their DoD point of contact and their "SPRS score.[35] Applicants can also provide CPO with evidence of purchase agreements from critical infrastructure customers, third-party certification to applicable industry standards, or a point of contact (e.g., a customer or federal employee) that can discuss sensitive or classified aspects of applicant's capabilities. CPO will work with applicants to verify information in a manner that meets any concerns regarding the exchange of sensitive information.

Finally, applicants can also provide to CPO 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. The plan could also address national security risks. For example, if an applicant partners with an entity that, according to DOC's Bureau of Industry and Security (BIS) participates in activities contrary to national security interests,[36] the applicant could take measures to isolate that entity from the funded project. Supply chain programs should be relevant to the customer(s) supported and applicable industry and U.S. government standards.

5.2 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 applicants to help projects "raise the bar" on security by identifying new practices for adoption related to foreign entities of concern, supply chain visibility and resilience, intellectual property protection, counterfeit mitigation, and cybersecurity.

[33] https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

[34] https://www.cisa.gov/topics.

[35] Supplier Performance Risk System. https://www.sprs.csd.disa.mil/default.htm

[36] https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list.

5.3 CPO's Security Framework

If selected for funding, CPO expects to work with applicants during the post-award, implementation phase 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.

CPO also encourages awardees' efforts to strengthen their security practices so that they will be positioned to pursue opportunities to support the defense and critical infrastructure sectors in the future. 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). Security practices that encompass each area of the CSF or are in line with the most current version of NIST SP 800-53, low-impact baseline, would be appropriate. CPO also expects that all funded projects will be capable of operating in the U.S. for an extended period of time without access to non-U.S. facilities and personnel. This could include, for example, onshoring of intellectual property, independent information system networks and maintenance personnel, and the appointment of U.S.-based security personnel, with sufficient skills and seniority, who are capable of implementing, monitoring, and controlling the security program of the applicant.

- **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. This could include a security and supply chain program that – in addition to implementing the low-impact baseline practices described above – is in line with industry-defined security and supply chain standards, requirements, or best practice guidance (e.g., automotive manufacturing security standards). Security practices that are in line with the most current version of NIST SP 800-53, moderate-impact baseline, along with controls 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. Supply chain programs should be relevant to the customer(s) supported and applicable industry and U.S. government standards.

- **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

[37] https://www.cisa.gov/resources-tools/resources/presidential-policy-directive-ppd-21-critical-infrastructure-security-and.

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 project-relevant security and supply chain requirements (e.g., maintaining a classified environment) and implementing the “medium bar” security and supply chain practices described above, security practices in line with the most current version of NIST SP 800-53, high-impact baseline, would be appropriate. Security and/or supply chain controls to prevent tampering and to mitigate insider threat, foreign influence, and supply chain risks would be important. A U.S.-based security program, staffed by appropriately skilled and senior security personnel, that can implement, monitor, and maintain the security program of the applicant may be necessary. Such a security program would need to be of sufficient size and maturity to mitigate potentially sophisticated risks that may be unique to each project. Supply chain programs should be relevant to the customer(s) supported and applicable industry and U.S. government standards.

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.

6. 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 can strengthen U.S. national security by producing a secure, reliable supply of semiconductors, especially for the defense industrial base 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 defense and critical infrastructure needs.

7. 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.)

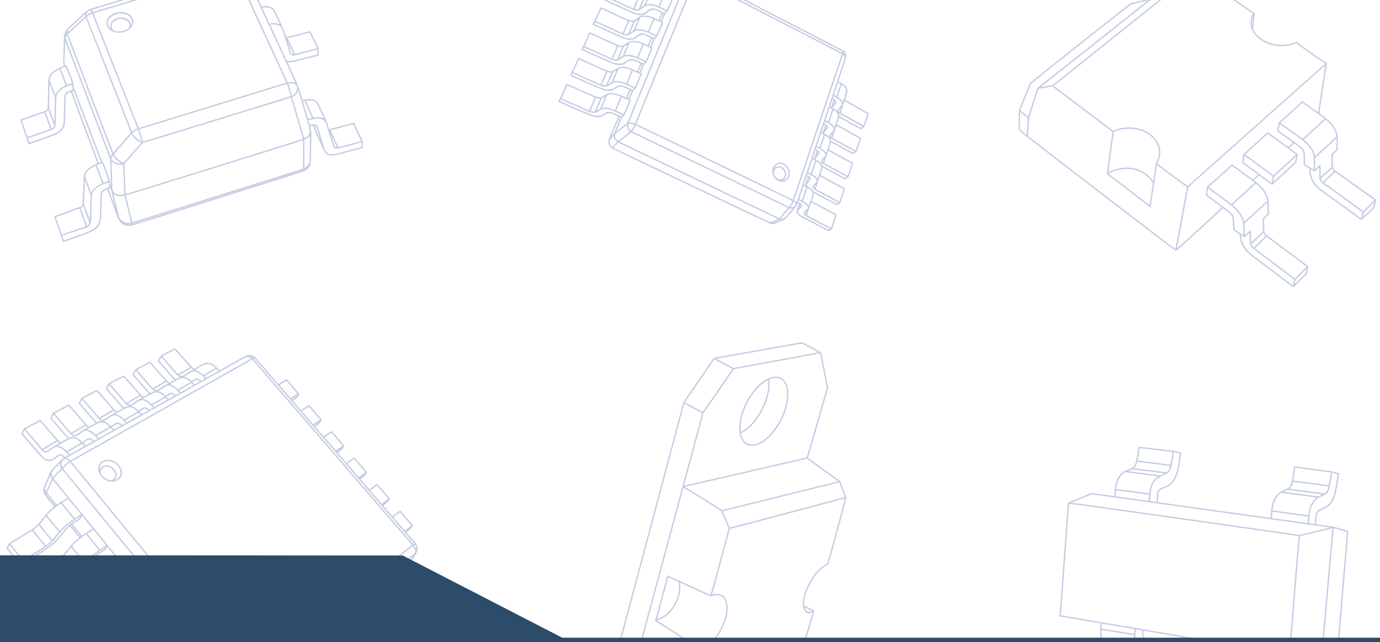
- **Network Segmentation** — An architectural approach that divides a network into multiple segments or subnets, each acting as its own small network allowing network administrators to control the flow of network traffic between subnets based on granular policies.

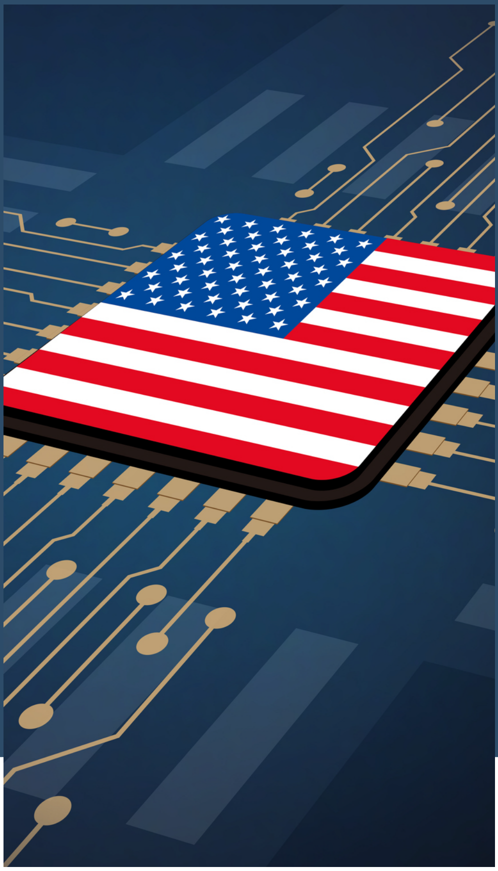
- **Redundant Capacity** — Additional capacity, bandwidth or other redundancies to limit the effects of information flooding denial-of-service attacks.

- **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.)





https://www.CHIPS.gov

askchips@chips.gov