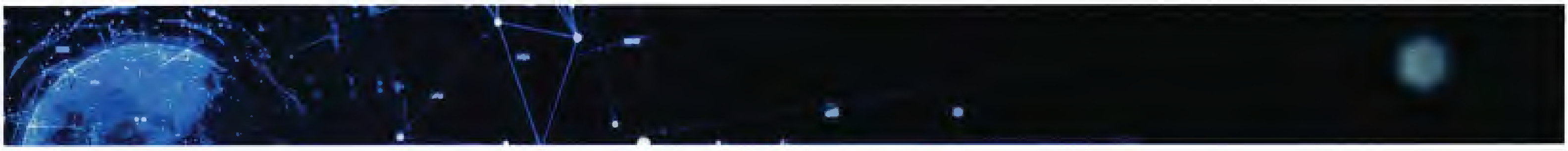
CLEARED
For Open Publication

Mar 21, 2024

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Defense Industrial Base Cybersecurity Strategy 2024



FOREWORD

The Department of Defense's (DoD) Defense Industrial Base (DIB) Cybersecurity Strategy is an actionable framework for sustaining a more resilient Joint Force and defense ecosystem—one that prevails within and through one of today's most contested domains: cyberspace.

Our nation's defense industrial base is critical to achieving our national security goals and maintaining our technology advantage. It is imperative that we protect it from the threat of malicious cyber activity and attacks. The Department has made tremendous strides in strengthening our overall cybersecurity and cyber resilience posture. In fact, many of the efforts underpinning this particular strategy have been underway for decades or more.

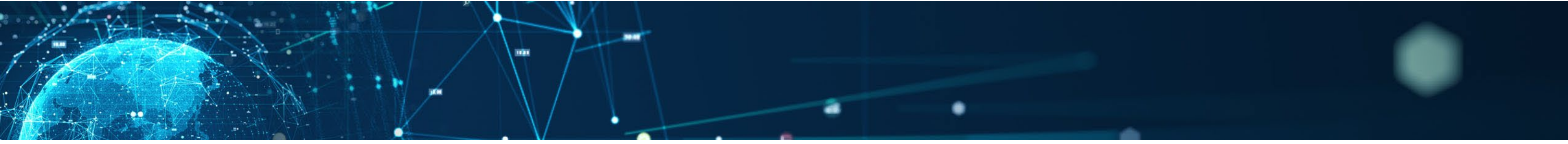
The DIB Cybersecurity Strategy ensures that we remain on the cutting edge of what it takes to secure our infrastructure. It requires us foremost to coordinate and collaborate across the Department to identify and close gaps in protecting our DIB networks, supply chains, and other critical resources. In it, we have identified opportunities where we can bolster the cybersecurity of the DIB, align the Department's focus on systemic challenges, and provide solutions that deliver the highest return on investment.

Figure 1: Deputy Secretary of Defense Kathleen H. Hicks speaks during the 2023 National Defense Industrial Association Conference, Washington, D.C., Aug. 28, 2023.

Moreover, we know that embracing a digital-first, data-driven culture and being customer-centric, agile, and flexible are key to driving the change we need. We must also continue to modernize our business practices, make appropriate investments in technology, and protect those investments by attracting and retaining a cyber workforce to meet the challenges of the current and future battlefield. Advancing these objectives and committing to the execution of this robust strategy will improve our overall cybersecurity and safeguard critical defense information. With teamwork and the right application of resources, this strategy will advance the Department's mission to defend the nation.

The Honorable Kathleen H. Hicks

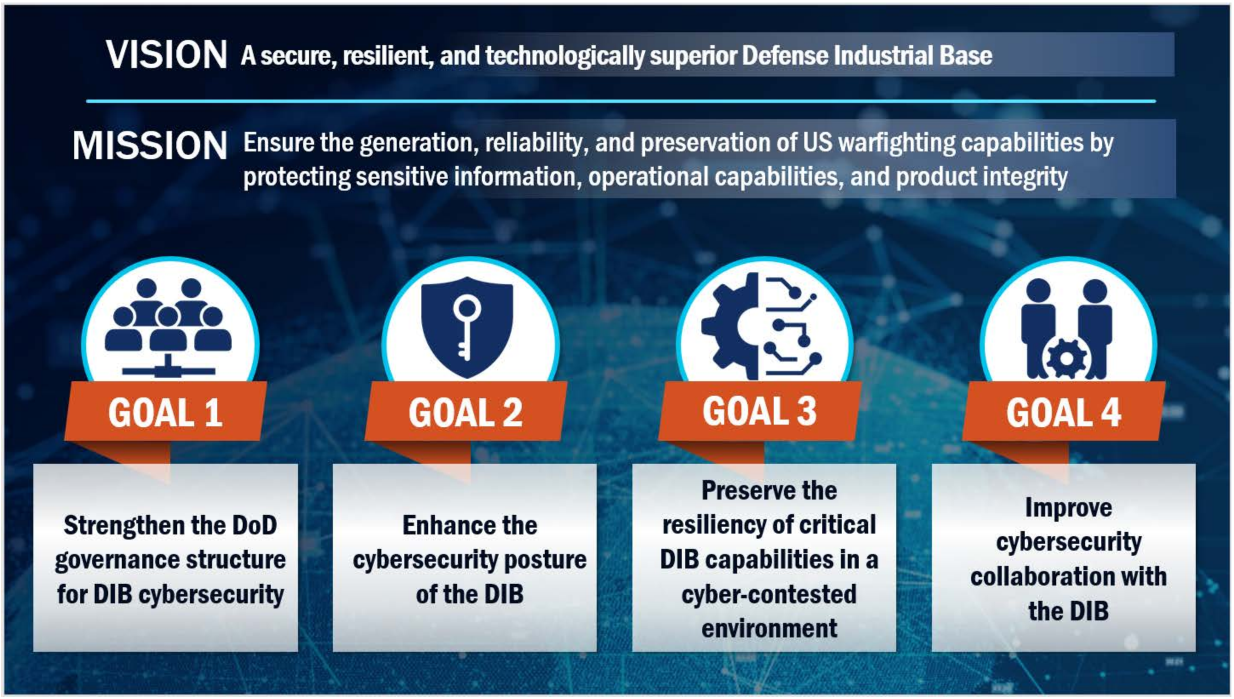
Deputy Secretary of Defense



EXECUTIVE SUMMARY

The DoD DIB Cybersecurity Strategy serves as the Department's strategic plan to enhance the cybersecurity and cyber resiliency of the DIB through an overarching vision and mission covering Fiscal Year (FY) 2024 through FY 2027. The Strategy outlines a set of four goals and their respective objectives that are aligned with interagency efforts and were developed by DoD stakeholders in coordination with the DIB to achieve a secure and resilient DIB information environment which promotes industry competitiveness, innovation, and sustainable growth. The Strategy supports the present and future needs of our Armed Forces and collaboration with the interagency and other key players in the cyberspace domain.

The Strategy nests under the *2022 National Defense Strategy* (NDS), the *2023 National Cybersecurity Strategy,* and the *2023 DoD Cyber Strategy* and alongside the *2024 DoD National Defense Industrial Strategy* (NDIS) and the National Institute of Standards & Technology (NIST) Cybersecurity Framework (CSF). In addition to the National and DoD strategies, this effort was informed by the Department's findings and response pursuant to Section 1648 of the National Defense Authorization Act (NDAA) for FY 2020 and Sections 1728 and 1737 of the NDAA for FY 2021.



VISION A secure, resilient, and technologically superior Defense Industrial Base

MISSION Ensure the generation, reliability, and preservation of US warfighting capabilities by protecting sensitive information, operational capabilities, and product integrity

GOAL 1 Strengthen the DoD governance structure for DIB cybersecurity

GOAL 2 Enhance the cybersecurity posture of the DIB

GOAL 3 Preserve the resiliency of critical DIB capabilities in a cyber-contested environment

GOAL 4 Improve cybersecurity collaboration with the DIB

Figure 2: FY 2024 – 2027 DoD DIB Cybersecurity Strategy

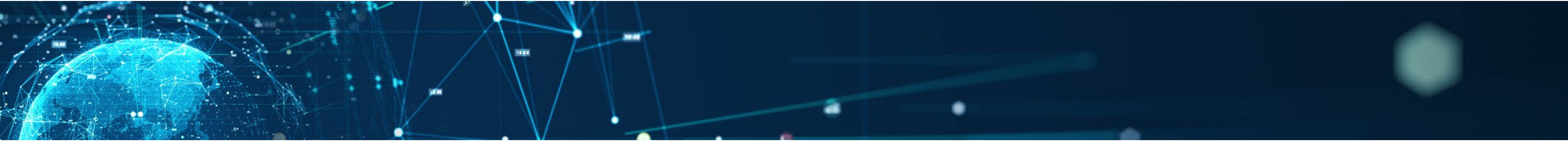


Table of Contents

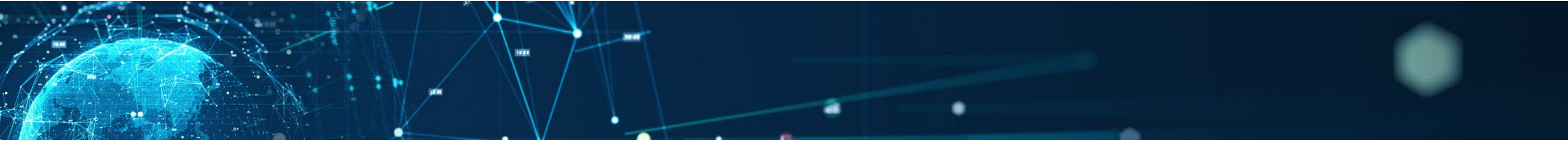
INTRODUCTION

The United States relies upon the ingenuity, hard work, and patriotism of the DIB to provide the necessary expertise, materiel, and infrastructure required to defend the Nation. As one of the sixteen critical infrastructure sectors identified in Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience,"[1] the DIB is the set of domestic and foreign companies or organizations—at all levels—that perform research and development, design, production, delivery, and maintenance of DoD systems, subsystems, and components or parts, as well as those who provide software and other critical services to meet U.S. defense requirements (see Appendix II). The Department of Defense relies upon the DIB to develop and produce innovative and highly advanced technologies so that, in conflict, the Department's warfighters have every available battlefield advantage when called to action in support of U.S. national security interests, and, in competition, the Department has the materiel needed for reliable production and delivery.

Figure 3: Soldiers don the Integrated Visual Augmentation System (IVAS) Capability Set 3 hardware while mounted in a Stryker at Joint Base Lewis-McCord, WA.

The Department relies upon the DIB to ensure the security of defense information residing on privately owned and operated information systems as well as the security of contractor proprietary information that underpins the innovative capabilities the U.S. Military needs to win decisively. The unauthorized access,

[1] Presidential Policy Directive – Critical Infrastructure Security and Resilience, White House, February 12, 2013, at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.



compromise, and theft of this vital information poses an imminent threat to U.S. national and economic security interests. The Department recognizes that the global networks in the DIB represent a foundational advantage in the cyberspace domain that must be protected and reinforced in harmonization with DoD's own.

The Department's reliance on the DIB to pursue technological advantages, provide critical support, and prevent unauthorized disclosure of sensitive information is not lost on our adversaries. DIB companies, both large and small, are at risk of malicious cyber activities conducted by foreign adversaries, such as Russia, China, Iran, and North Korea, in addition to nonstate actors, such as violent extremist organizations and transnational criminal organizations. With the goal of espionage or sabotage, and sometimes both, malicious cyber activity targeting the DIB can result in the unauthorized access and release of sensitive U.S. Government (USG) data, proprietary information, and intellectual property, as well as the destruction of data, inability to conduct business, denial of services, and physical damage to property.

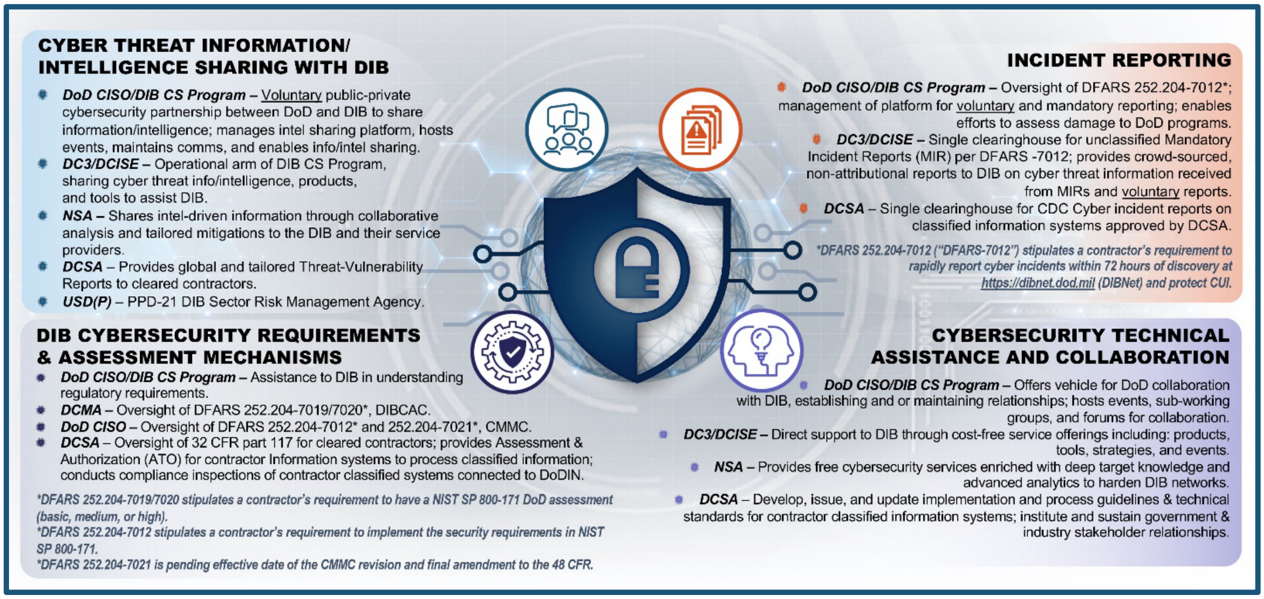
Unauthorized access to DIB systems and networks by foreign adversaries not only provides a means to collect intelligence, steal trade secrets, and leapfrog over generations of research and development, but it also informs the future targeting of critical infrastructure vulnerabilities, manipulation of public information for strategic communication objectives, and other follow-on cyber operations. More broadly, as Deputy Secretary of Defense (DSD) Kathleen Hicks has stated, these cyber-attacks "threaten the U.S. and the rules-based order on which the global economy relies." Markets cannot function effectively in an environment where adversarial countries are leveraging national power to steal intellectual property, sabotage commercial activity, and threaten supply chains.[2]

Today, the Department delineates the roles and responsibilities for DIB cybersecurity across several components, chief among these being the Under Secretary of Defense for Research and Engineering (USD(R&E)), the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), the Under Secretary of Defense for Policy (USD(P)), the Under Secretary of Defense for Intelligence and Security (USD(I&S)), and the DoD Chief Information Officer (CIO). Responsibilities for DIB cybersecurity are further sub-divided among the National Security Agency (NSA), the DoD Cyber Crime Center (DC3), the Defense Counterintelligence and Security Agency (DCSA), United States Cyber Command (USCYBERCOM), and the Chief Information Security Officers and Program Managers of the Military Departments and Combatant Commands.

To encourage cybersecurity best practices in the DIB, the Department employs a multi-pronged approach that includes establishing public-private cooperatives such as the voluntary DoD DIB Cybersecurity Program;[3] contributing to, amplifying, and adopting NIST standards, frameworks, and guidance; and working with industry associations on cybersecurity, training, and implementation while keeping DIB contractor identifying information anonymous. The *National Cybersecurity Strategy* considers "robust collaboration, particularly between public and private sectors" as "essential to securing cyberspace."[4] The

[2] "DOD Focused on Protecting the Defense Industrial Base from Cyber Threats," David Vergan, *DoD News*, February 7, 2022, at https://www.defense.gov/News/News-Stories/Article/Article/2926539/dod-focused-on-protecting-the-defense-industrial-base-from-cyber-threats/.
[3] The DoD DIB Cybersecurity Program is established in Part 236 of Title 32, Code of Federal Regulations (CFR), *DoD DIB Cybersecurity Activities*, at https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-M/part-236.
[4] *National Cybersecurity Strategy*, p. 2, White House, March 2023, at https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

Department, in coordination with the DIB, seeks to build upon and improve the combination of regulations, policies, requirements, programs, services, pilots, communities of interest, public-private cooperatives, and interagency efforts to achieve a more cyber-secure and resilient DIB.



CYBER THREAT INFORMATION/ INTELLIGENCE SHARING WITH DIB

- ***DoD CISO/DIB CS Program*** – Voluntary public-private cybersecurity partnership between DoD and DIB to share information/intelligence; manages intel sharing platform, hosts events, maintains comms, and enables info/intel sharing.
- ***DC3/DCISE*** – Operational arm of DIB CS Program, sharing cyber threat info/intelligence, products, and tools to assist DIB.
- ***NSA*** – Shares intel-driven information through collaborative analysis and tailored mitigations to the DIB and their service providers.
- ***DCSA*** – Provides global and tailored Threat-Vulnerability Reports to cleared contractors.
- ***USD(P)*** – PPD-21 DIB Sector Risk Management Agency.

DIB CYBERSECURITY REQUIREMENTS & ASSESSMENT MECHANISMS

- ***DoD CISO/DIB CS Program*** – Assistance to DIB in understanding regulatory requirements.
- ***DCMA*** – Oversight of DFARS 252.204-7019/7020*, DIBCAC.
- ***DoD CISO*** – Oversight of DFARS 252.204-7012* and 252.204-7021*, CMMC.
- ***DCSA*** – Oversight of 32 CFR part 117 for cleared contractors; provides Assessment & Authorization (ATO) for contractor Information systems to process classified information; conducts compliance inspections of contractor classified systems connected to DoDIN.

***DFARS 252.204-7019/7020 stipulates a contractor's requirement to have a NIST SP 800-171 DoD assessment (basic, medium, or high).*
***DFARS 252.204-7012 stipulates a contractor's requirement to implement the security requirements in NIST SP 800-171.*
***DFARS 252.204-7021 is pending effective date of the CMMC revision and final amendment to the 48 CFR.*

INCIDENT REPORTING

- ***DoD CISO/DIB CS Program*** – Oversight of DFARS 252.204-7012*; management of platform for voluntary and mandatory reporting; enables efforts to assess damage to DoD programs.
- ***DC3/DCISE*** – Single clearinghouse for unclassified Mandatory Incident Reports (MIR) per DFARS -7012; provides crowd-sourced, non-attributional reports to DIB on cyber threat information received from MIRs and voluntary reports.
- ***DCSA*** – Single clearinghouse for CDC Cyber incident reports on classified information systems approved by DCSA.

***DFARS 252.204-7012 ("DFARS-7012") stipulates a contractor's requirement to rapidly report cyber incidents within 72 hours of discovery at https://dibnet.dod.mil (DIBNet) and protect CUI.*

CYBERSECURITY TECHNICAL ASSISTANCE AND COLLABORATION

- ***DoD CISO/DIB CS Program*** – Offers vehicle for DoD collaboration with DIB, establishing and or maintaining relationships; hosts events, sub-working groups, and forums for collaboration.
- ***DC3/DCISE*** – Direct support to DIB through cost-free service offerings including: products, tools, strategies, and events.
- ***NSA*** – Provides free cybersecurity services enriched with deep target knowledge and advanced analytics to harden DIB networks.
- ***DCSA*** – Develop, issue, and update implementation and process guidelines & technical standards for contractor classified information systems; institute and sustain government & industry stakeholder relationships.

Figure 4: Current DoD DIB Cybersecurity Efforts

At the national level, the DoD fulfills its duties with respect to the Federal Information Security Modernization Act[5] by implementing programs that bolster protection of federal information residing on government and non-government networks. These programs align with the requirements of the controlled unclassified information (CUI) program established by Executive Order (EO) 13556.[6] Additionally, the Department executes responsibilities associated with PPD-21 as the Sector Risk Management Agency (SRMA) responsible for improving the security and resilience of the DIB, and EO 14028 of May 12, 2021, that requires government agencies to, among other actions, update contracting language on collecting and preserving cybersecurity event data and sharing it government-wide.

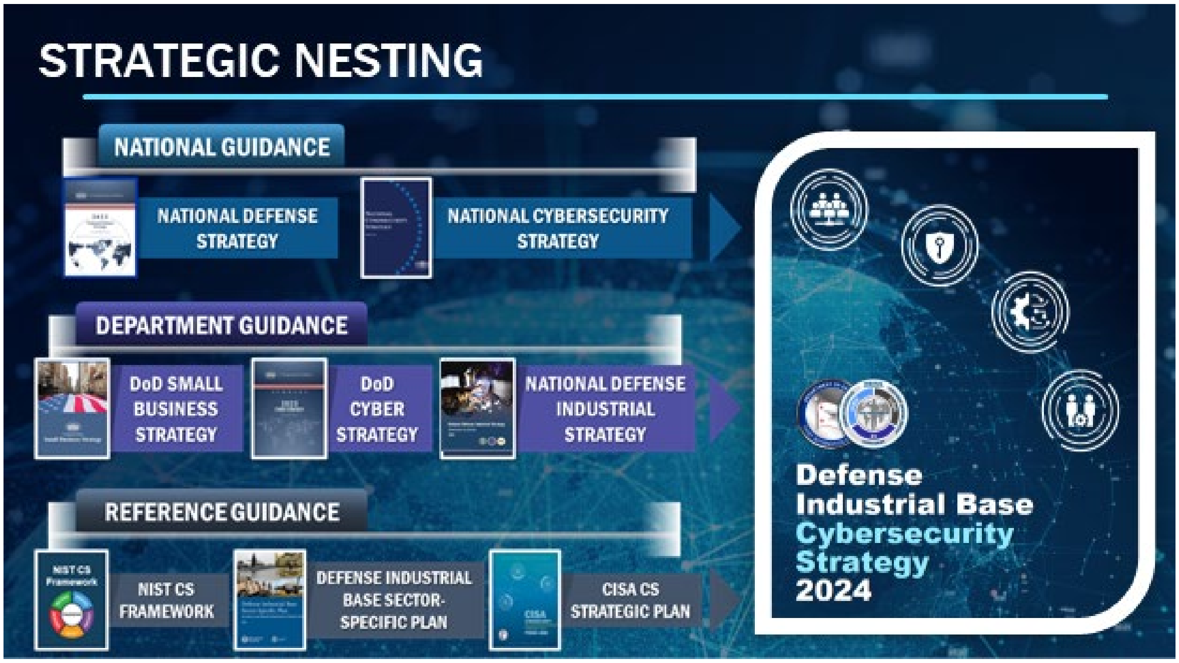
To address current and future challenges, the Department is publishing this Strategy to guide its response to the ever-evolving cyber threats facing the DIB. This Strategy will inform subsequent updates to DoD's Sector-Specific Plan (SSP), as required by the National Infrastructure Protection Plan and PPD-21. In this Strategy, the Department will build upon lessons learned and successes working with the DIB on cybersecurity concerns related to the protection of federal information and expand collaboration to include availability and integrity needed to ensure continuity of operations for critical DIB suppliers in the defense of the Nation and support of its warfighters. The Department stands firm in its commitment to bolster the DIB against current threats and work toward long-term solutions to make the cyberspace domain more defensible and resilient in the future.

[5] Public Law No: 113-283, Federal Information Security Modernization Act of 2014, at https://www.congress.gov/bill/113th-congress/senate-bill/2521.
[6] EO 13556 – Controlled Unclassified Information, White House, November 4, 2010, at https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information.

Figure 5: US Navy Lt. James Dubyoski and Naval Postgraduate School (NPS) assistant professor Tony Pollman conduct testing on the Disposable Reusable Expeditionary Warfare Underwater Vehicle (DREW UV) in collaboration with Naval Surface Warfare Center, Panama City, FL. The Naval Innovation Center at the NPS will solve complex challenges through applied research, analysis, prototyping, and experimentation in collaboration with the DIB, the technology sector, and academia.

STRATEGIC ALIGNMENT

The *DoD DIB Cybersecurity Strategy* aligns with guidance presented in the 2022 NDS, the *2023 National Cybersecurity Strategy*, the *2023 DoD Cyber Strategy*, the *Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Strategic Plan*,[7] and the *DoD Small Business Strategy*.[8] This Strategy supports DoD Components and DIB contractors more fully integrating the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (NIST CSF)[9] into DIB operating plans and the execution of cybersecurity responsibilities.



STRATEGIC NESTING

NATIONAL GUIDANCE

NATIONAL DEFENSE STRATEGY

NATIONAL CYBERSECURITY STRATEGY

DEPARTMENT GUIDANCE

DoD SMALL BUSINESS STRATEGY

DoD CYBER STRATEGY

NATIONAL DEFENSE INDUSTRIAL STRATEGY

REFERENCE GUIDANCE

NIST CS FRAMEWORK

DEFENSE INDUSTRIAL BASE SECTOR-SPECIFIC PLAN

CISA CS STRATEGIC PLAN

Defense Industrial Base Cybersecurity Strategy 2024

Figure 6: DoD DIB Cybersecurity Strategic Alignment

- ➢ The 2022 NDS establishes the mandate for integrated deterrence against strategic attacks on the United States and its allies and partners to build a resilient Joint Force and defense ecosystem.[10] This Strategy focuses the combined, collaborative efforts of the defense ecosystem to bolster the cybersecurity of the Department, the DIB, and the array of private sector and academic enterprises that create and sharpen the Joint Force's technological edge.

- ➢ Pursuant to guidance put forth in the *2023 National Cybersecurity Strategy*, this Strategy aims to use a whole-of-government approach to disrupt malicious cyber activity at scale[11] and fortify the cybersecurity of the DIB as increasingly capable adversaries adopt tactics to undermine U.S. national interests.

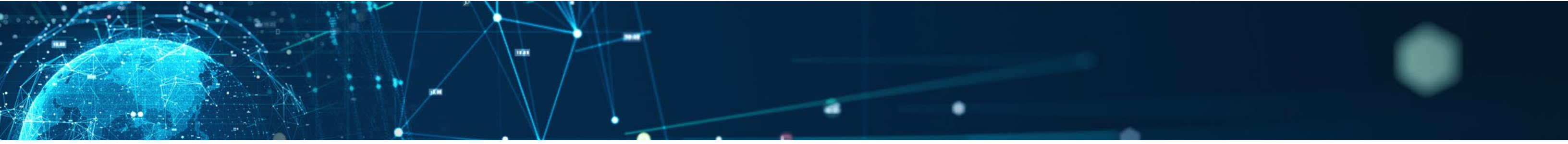
[7] *CISA Cybersecurity Strategic Plan FY2024-2026*, CISA, August 2023, at https://www.cisa.gov/sites/default/files/2023-08/FY2024-2026_Cybersecurity_Strategic_Plan.pdf.

[8] *Small Business Strategy*, DoD, January 2023, at https://media.defense.gov/2023/Jan/26/2003150429/-1/-1/0/SMALL-BUSINESS-STRATEGY.PDF.

[9] *Framework for Improving Critical Infrastructure Cybersecurity*, ver. 1.1, NIST, April 16, 2018, at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[10] *National Defense Strategy*, DoD, 2022, p. 1.

[11] *National Cybersecurity Strategy*, Strategic Objective 2.1, p. 14.



- The Department's collaboration with the DIB, much of which is comprised of small businesses, means helping the DIB secure itself against cybersecurity threats of increasing frequency and severity.[12] In alignment with the *DoD Small Business Strategy* and a truly integrated deterrence, this strategy will improve the sharing of cybersecurity resources available to the DIB for the purpose of educating and enabling DIB companies to understand how best to safeguard DIB systems and improve resiliency. This Strategy also addresses the need to improve the effectiveness of cybersecurity regulations, policies, and requirements.

- In accordance with the *2023 DoD Cyber Strategy*, the objectives of this Strategy aim to fulfill the requirement for the Department to continue leveraging public-private cooperation and supporting investment in rapid information-sharing and analysis. It responds directly to the requirement to "develop a comprehensive approach for the identification, protection, detection, response, and recovery of critical DIB elements, thereby ensuring the reliability and integrity of critical weapons systems and production nodes."[13]

- This Strategy aligns with the priorities of the 2024 NDIS to expand resources for small businesses, increase vulnerability mitigation and supply chain resilience, and strengthen enforcement against cyber-attacks.

- This Strategy is informed by the NIST CSF, a voluntary set of standards, guidelines, and practices published by NIST in coordination with stakeholders, including private industry. A direct consequence of the 2013 EO 13636, *Improving Critical Infrastructure Cybersecurity*,[14] the NIST CSF is the primary framework the Department recommends for both public and private sector organizations to reference when managing and reducing cybersecurity risks. DoD's Cybersecurity Reference Architecture incorporates the NIST CSF, the Joint Capability Area taxonomy, the MITRE ATT&CK® Framework, and the MITRE D3FEND™ Framework to describe and provide supporting rationale for the capabilities that should be present in the architecture. The Department continues to lead by example with the adoption of the CSF and provision of educational opportunities to the DIB on its applicability to other information environments.

- Cybersecurity is identified by the DIB SSP[15] as "arguably the most urgent infrastructure protection issue facing the Nation." This Strategy is a step towards the DoD goal outlined in the DIB SSP of securing cyberspace and setting conditions for long-term success.

- Finally, CISA's *Cybersecurity Strategic Plan FY2024 – 2026* outlines goals and objectives that are in alignment with the *DoD DIB Cybersecurity Strategy*. CISA aims to drive mitigation of exploitable vulnerabilities, improve cybersecurity capabilities, and promote the continued implementation of cybersecurity investments.

[12] *DoD Small Business Strategy*, Strategic Objective 3.2.

[13] 2023 *DoD Cyber Strategy* Summary, DoD, p. 8, at https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF.

[14] EO 13636, *Improving Critical Infrastructure Cybersecurity*, White House, February 12, 2013, at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[15] *Defense Industrial Base Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Department of Homeland Security and the Department of Defense, 2010.

GOALS AND OBJECTIVES

The cybersecurity of the DIB is critical to the success of the Department's national security mission. Protecting DIB contractor information environments from malicious cyber activity is no less consequential than protecting those of the Department of Defense. By protecting sensitive information, operational capabilities, and product integrity in the DIB, the Department will better achieve the generation, reliability, and preservation of U.S. warfighting capabilities.

In support of this mission, the Department will seek to achieve four primary goals in coordination with numerous components, Program Managers, and the DIB. Many of the efforts underpinning the objectives noted in this strategy have already begun or have been an element of the Department's approach to DIB cybersecurity spanning decades or more. This Strategy aims to sharpen the focus, collaboration, and integration of these efforts, ultimately improving the resiliency of the defense cybersecurity ecosystem.

VISION A secure, resilient, and technologically superior Defense Industrial Base

MISSION Ensure the generation, reliability, and preservation of U.S. warfighting capabilities by protecting sensitive information, operational capabilities, and product integrity

GOAL 1

STRENGTHEN THE DOD GOVERNANCE STRUCTURE FOR DIB CYBERSECURITY

OBJECTIVES

1.1: Strengthen interagency collaboration for cross-cutting cybersecurity issues

1.2: Advance the development of regulations governing cybersecurity responsibilities of DIB contractors and subcontractors

GOAL 2

ENHANCE THE CYBERSECURITY POSTURE OF THE DIB

OBJECTIVES

2.1: Evaluate DIB compliance with DoD's cybersecurity requirements

2.2: Improve the sharing of threat, vulnerability, and cyber-related intelligence with the DIB

2.3: Identify vulnerabilities in DIB IT cybersecurity ecosystems

2.4: Recover from malicious cyber activity

2.5: Evaluate the effectiveness of cybersecurity regulations, policies, and requirements

GOAL 3

PRESERVE THE RESILIENCY OF CRITICAL DIB CAPABILITIES IN A CYBER-CONTESTED ENVIRONMENT

OBJECTIVES

3.1: Prioritize the cyber resiliency of critical DIB production capabilities

3.2: Establish in policy the priority focus on cybersecurity for critical suppliers and facilities

GOAL 4

IMPROVE CYBERSECURITY COLLABORATION WITH THE DIB

OBJECTIVES

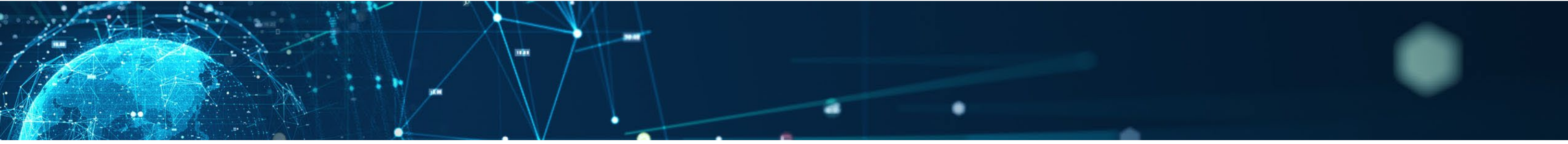
4.1: Leverage collaboration with commercial internet, cloud, and cybersecurity service providers to enhance DIB cyber threat awareness

4.2: Work with the DIB SCC to improve communication and collaboration with the DIB

4.3: Improve bidirectional communication with the DIB and expand public-private cybersecurity collaboration

GOAL 1. Strengthen the DoD governance structure for DIB cybersecurity

Securing DIB cyberspace requires numerous offices and agencies to coordinate and authorities to align for the synchronization of supporting objectives and activities. The DSD endorsed updating the Department's objectives, requirements, resourcing, and roles and responsibilities for DIB cybersecurity in February 2022. To meet this challenge, the DoD CIO called on the DIB Cybersecurity Executive Steering Group (ESG) to develop strategies to improve the cybersecurity of the DIB. Realizing that the Department's responsibilities concerning the DIB are broadly distributed, the Department seeks to strengthen the internal governance structure for DIB activities.



Objective 1.1 Strengthen interagency collaboration for cross-cutting cybersecurity issues

Diverse interagency stakeholder groups face many of the same cybersecurity issues, from growing risk awareness to designing and implementing strategies to improve cybersecurity and aiding the DIB in recovery from malicious cyber activity. This Strategy seeks to foster joint efforts and enhance communication across the DIB cybersecurity community.

Government stakeholders, internal and external to the Department, must collaborate to bolster DIB cybersecurity. The DoD CISO chairs the DIB Cybersecurity ESG to develop and coordinate policies and guidance to further the protection of DIB contractor information environments. The DoD CIO oversees the DoD DIB Cybersecurity Program, which serves as the central hub for shaping and implementing a DoD-wide strategic approach to improving DIB cybersecurity. The DoD CIO also works in harmony with the Office of the USD(R&E), which oversees the Office of the Secretary of Defense (OSD) Damage Assessment Management Office (DAMO), a nexus between the DoD DIB Cybersecurity Program and DIB cyber incident reporting, all collocated with DC3. USD(P), in turn, manages risk via DoD's Mission Assurance construct and chairs the DIB Government Coordinating Council (GCC) to convene and coordinate stakeholders and shape, align, coordinate, and facilitate communication on policy and programmatic efforts to improve DIB security and resilience.

The Department may also execute its DIB cybersecurity responsibilities as part of broader federal responses to cyber risks, threats, or incidents involving the DIB. In these cases, actions from law enforcement/counterintelligence agencies (LE/CIs), the Department of Homeland Security (DHS), and CISA may all take place in concert to secure the DIB cyberspace domain. Under the auspices of the DHS Critical Infrastructure Partnership Council (CIPAC), NSA participates in the Enduring Security Framework—a public-private cooperative comprised of DoD and the DIB established to work on shared cybersecurity challenges. These stakeholders must collaborate to assess the current risk environment, outline the nexus between cyber and information security, as well as cyber and physical security, and address the interdependence between the DIB sector and other critical infrastructure and critical program and technology sectors.

While this Strategy aims to protect the DIB, both on and off DoD Information Networks (DODIN), by providing integrated deterrence for known and emerging threats and vulnerabilities, the tactics and tools utilized by a determined malicious cyber actor may require an even more robust response. The Department may need to coordinate such a response as part of a larger interagency and/or state, local, tribal, and territorial (SLTT) response if the situation necessitates a transition from proactive cybersecurity to executing a defense within cyberspace when there is risk to critical infrastructure or national interests. In these instances, the response may include coordinated actions from the Department, other federal LE/CIs, CISA, and USCYBERCOM. Conducting a successful defense within cyberspace is founded upon the establishment of a forum that facilitates that coordination and reduces the gaps and seams between the Department and the rest of the government. For FYs 2024-2027, the Department seeks to mature the cross-departmental mechanisms for a coordinated response to managing cyber risk.

DOD STAKEHOLDER: The DoD CIO is responsible for informing policies that expand cyber threat information-sharing and provide cybersecurity services to the DIB (e.g., DoD DIB Cybersecurity Program), developing and overseeing implementation of the Cybersecurity Maturity Model Certification (CMMC) program, and restricting unnecessary sharing of sensitive information during system or platform development.

Figure 8: A US Cyber Command member works in the Integrated Cyber Center/Joint Operations Center at Fort George G. Meade, MD.

Objective 1.2 Advance the development of regulations governing cybersecurity responsibilities of DIB contractors and subcontractors

Executing a comprehensive and dynamic cybersecurity program requires the development of regulations to evaluate and strengthen cybersecurity requirements for the DIB. The contractually mandated cybersecurity requirements from Defense Federal Acquisition Regulation Supplement (DFARS) 252.204–7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting;"[16] DFARS 252.204-7020, "NIST SP 800-171 DoD Assessment Requirements;"[17] and DFARS 252.239-7010, "Cloud Computing Services,"[18] are an important part of the DIB cybersecurity ecosystem.[19] DFARS 252.204-7012 requires that NIST 800-171 cybersecurity requirements are applicable to subcontractors; however,

[16] DFARS 252.204–7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," at https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.

[17] DFARS 252.204-7020, "NIST SP 800-171 DoD Assessment Requirements," at https://www.acquisition.gov/dfars/252.204-7020-nist-sp-800-171dod-assessment-requirements.

[18] DFARS 252.239-7010, "Cloud Computing Services," at https://www.acquisition.gov/dfars/252.239-7010-cloud-computing-services.

[19] DFARS directs DIB contractors and suppliers to NIST Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," and the "Cloud Computing Security Requirements Guide" as a cybersecurity requirement for DIB contractors that process, transmit, and store CUI.

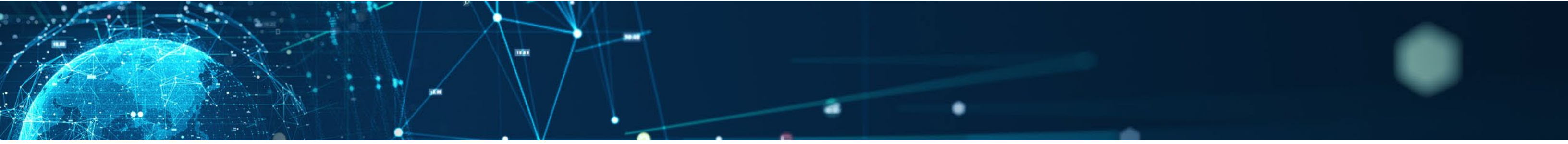
visibility within the lower tiers remains a challenging area for the Department. Regulations governing the flow-down of cybersecurity requirements for DIB subcontractors is an evolving and shared responsibility which leverages numerous stakeholders in pursuit of the guidance and processes to establish, mature, and maintain cybersecurity best practices applicable at the lower tiers. For FYs 2024-2027, the Department will work with the DIB, and interagency and DoD stakeholders to build a governance framework for maintaining a secure subcontractor cybersecurity environment.

Figure 9: Government employees, service members, industry, academia, and vendors interact in the exhibit hall during the 2023 Innovation Industry Days at the Henry B. Gonzalez Convention Center on January 24, 2023. The collider event, a partnership between the Air Force Installation and Mission Support Center and AFWERX, gave Airmen and Guardians an opportunity to network with industry and academia to hear about successes, failures, and lessons learned to help identify paths for implementing solutions for their mission needs.

GOAL 2.
Enhance the cybersecurity posture of the DIB

Maintaining technology advantage largely depends upon ensuring appropriate protection of domestic proprietary information and production capability and those of U.S. allies and partners. A key element of protecting proprietary information is encouraging DIB adoption of voluntary cybersecurity best practices alongside certifying compliance with contractual cybersecurity requirements and routine testing of cybersecurity systems. Based on evolving threats, the Department recognizes the need for some DIB contractors to further enhance their cybersecurity posture to address advanced persistent threats (APTs).

The Department also acknowledges the need to work with DIB contractors on ways to enhance protections for availability and integrity of certain systems where loss of proprietary information or DoD data is not the key driver of technology advantage, but the availability of that capability is critical to national security. Robust cybersecurity may be achieved through iterative risk assessments and mitigation of gaps in security posture combined with facilitating DIB contractor adherence to cybersecurity regulations. A multitude of concurrent activities are required to avoid the loss or disruption of critical facilities and any associated program or technologies. The Department will engage with the DIB in conducting gap assessments, providing training and other resources, and incorporating DIB feedback. Alongside the sharing of cybersecurity best practices and quick adoption of evolving standards and guidelines, these efforts require continued collaboration between the Department, the DIB, and NIST among other government and non-federal partners.



Objective 2.1 Evaluate DIB compliance with DoD's cybersecurity requirements

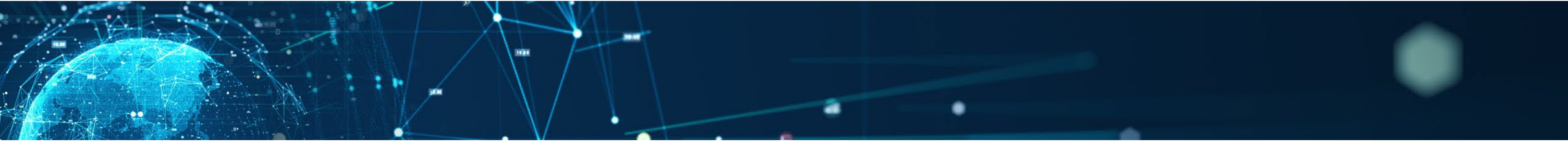
DOD STAKEHOLDER: The Defense Contract Management Agency (DCMA) DIB Cybersecurity Assessment Center (DIBCAC) plays a significant role in executing DoD's contractor cybersecurity risk mitigation efforts. The DIBCAC assesses DoD contractors' compliance with DFARS 252.204-7012, and NIST SP 800-171 in accordance with DFARS 252.204-7020.

Evaluating compliance with DoD security requirements, as specified in FAR 52.204-21, or DFARS 252.204-7012, is an important aspect of understanding and subsequently investing in efforts to improve the cybersecurity of DIB contractors. Today, the Department conducts contractually required Medium or High NIST SP 800-171 DoD Assessments only for prioritized DIB contractors to verify overall compliance with DFARS 252.204-7012 and implementation of NIST SP 800-171 requirements. In the future, the Department will continue to do so through the CMMC program, which will establish a large-scale verification capability, allowing self-assessment for some requirements, leveraging independent assessments on DIB companies that will receive CUI associated with the Department's programs, conducting assessments on the subset of DIB companies that will receive CUI associated with the Department's most critical and sensitive programs and technologies, and reinforcing cooperation between the Department and industry in addressing evolving cyber threats. Results of CMMC and DoD High and Medium assessments must be posted in the Supplier Performance Risk System to meet contract eligibility requirements.

DOD STAKEHOLDER: Within the DoD CIO, the CMMC Program will significantly expand the quantity of independent assessments of the DIB using Commercial Third-Party Assessment Organizations and will enhance the DIB's protection against APTs by requiring new DoD assessments based on NIST SP 800-172 requirements.

The increasing number of threats resulting from the evolution and expansion of the digital ecosystem drives the need for enhanced requirements for a subset of critical programs or high value assets. Future rulemaking efforts will expand existing information safeguarding requirements for these companies by implementing supplemental guidelines defined in NIST SP 800-172, "Enhanced Security Requirements for Protecting Controlled Unclassified Information." While DFARS specifies the minimum DIB cybersecurity requirements for companies that process, transmit, and store CUI, the Department must also support efforts by the DIB to make risk-informed decisions to exceed these requirements.

The Department will also conduct voluntary cybersecurity readiness assessments of DIB contractors' policies and controls to ascertain their cybersecurity posture or facilitate self-assessments. DC3 provides an ongoing service to DoD DIB Cybersecurity Program participants to assess cybersecurity readiness. Through the Cyber Resilience Analysis (CRA) service, DC3 facilitates a government assessment as well as provides support for a self-assessment. Any DIB contractor data used in the CRA program is not shared. These assessments help the DIB contractor understand where to allocate resources more effectively to address any gaps.



To support the enhanced requirements found in NIST SP 800-172,[20] DC3 is now conducting Adversary Emulation Tests (AET) as a standing service offering. AETs are a more invasive threat-informed penetration test, or assessment, of a DoD DIB Cybersecurity Program participant's network and systems that store, process, or transmit Covered Defense Information (CDI). The data from CRA and AET participation is also used to inform DC3 threat and vulnerability mitigation information products that are provided exclusively to companies participating in the DoD DIB Cybersecurity Program.

DOD STAKEHOLDER: DC3 is a Federal Cyber Center providing cyber threat analytics and threat information sharing with a range of DIB and USG partners. As the single focal point and data repository for DIB cyber incident reporting, DC3-maintains and shares data with DoD and USG partners and generates leads for LE/CI investigations and operations, resulting in administrative, civil, and criminal penalties for entities that pose threats to the DIB. DC3 also enriches DIB reporting with all-source intelligence analysis and disseminates this information via various intelligence products, reports, and actor profiles to enable a broad range of actions against malicious cyber actors. DC3 manages the DoD-Defense Industrial Base Collaborative Information Sharing Environment (DCISE), which is the operational hub of the DoD DIB Cybersecurity Program.

Objective 2.2 Improve the sharing of threat, vulnerability, and cyber-related intelligence with the DIB

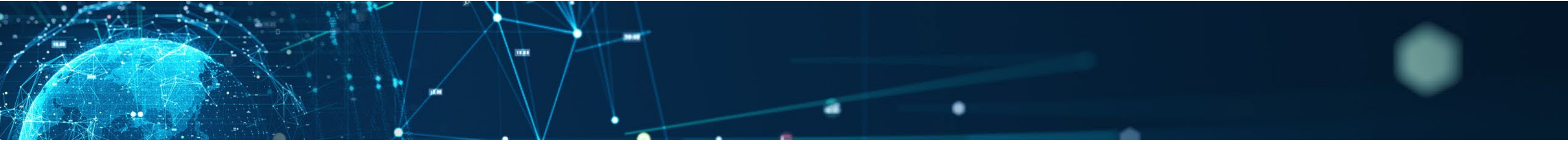
Bolstering the cybersecurity of DIB assets requires the ability to disseminate relevant and timely threat information, to include coordination with international partners and allies, as appropriate. The Department executes the DoD DIB Cybersecurity Program as the focal point for engagement today with cleared defense contractors to better secure unclassified networks, with expectations to expand in the near future to all DIB contractors handling CUI. The DoD DIB Cybersecurity Program is a public-private cybersecurity cooperative for sharing unclassified and classified cyber threat information to advance a near real-time picture of the current threat environment and support participants' capabilities to safeguard defense and DIB information residing on or transiting DIB unclassified information systems. The Department disseminates alerts and warnings to notify the DIB of critical, time-sensitive information through DIBNet[21]. The DoD CIO will oversee a relaunch of the DIBNet Portal in FY 2024 to continue the evolution of threat sharing capabilities. A key feature of the new system will be the application programming interface-based retrieval of threat information.

DOD STAKEHOLDER: Commander, USCYBERCOM, is delegated authority to enter arrangements with willing private sector entities to share threat information related to malicious cyberspace actors and activities associated with a determination that the Russian Federation, the PRC, the DPRK, or Iran is conducting an active, systemic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace.

DC3, in close cooperation with Defense Criminal Investigation Organizations and Military Department Counterintelligence Organizations, is developing the DoD framework to provide information sharing of data to enhance cyber-CI investigations and operations. Composed of physical and virtualized sensors utilizing leading-edge technologies, the Collect, Analyze, Disseminate, and Operationalize - Integrated

[20] NIST SP 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information, A Supplement to NIST Special Publication 800-171*, NIST, February 2021, at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172.pdf.

[21] DIBNet Portal is located at https://dibnet.dod.mil.



Solution (CADO-IS) is a scalable cyber defense solution that leverages machine learning and deep learning technologies, advanced analytics, and rule-based detection to identify malicious cyber activity. CADO-IS will enhance cyber defense capabilities for major weapons systems, critical defense technologies and infrastructure, and research efforts. After completing DoD-wide requirements capture and initial technical planning, CADO-IS identified technology breakthroughs using a new cloud-based design and implemented initial fielding of an exfil database to DoD CI entities. Future efforts include integration with DIB cybersecurity data, USCYBERCOM operations, and other data and capabilities at scale.

To expand upon current capabilities that proactively and retroactively analyze DoD DIB Cybersecurity Program participant organizational systems, networks, and infrastructure for malicious cyber activity, DC3 will utilize an existing service offering called "DCISE Cubed," and future complimentary tools. DCISE Cubed is a firewall log analysis capability that automatically scores connections to DIB networks utilizing cyber threat information and collected indicators. Once scored, connections identified as malicious are flagged for recommended courses of action that may include blocking on the DIB infrastructure (or network). DCISE Cubed utilizes open source, commercial, and USG cyber threat information feeds to provide insights on cyber activity impacting the DIB.

NSA engages with DIB organizations to share non-public, DIB-specific threat intelligence to help prevent, detect, and mitigate malicious cyber activity. For those DIB organizations, the Cybersecurity Collaboration Center (CCC) opens a secure collaboration channel that allows for DIB network defenders to submit questions and feedback on findings related to the threat intelligence NSA shares directly back to the analysts to further inform analysis and communicate with the broader DoD and DIB communities for awareness when needed. By leveraging its technical expertise and capability, and its unique insights on nation-state cyber threats, malware, tactics, techniques, and procedures, NSA also develops public advisories and mitigations on evolving cybersecurity threats designed to defend the Nation.

Objective 2.3 Identify vulnerabilities in DIB information technology (IT) cybersecurity ecosystems

While carrying out its missions, the USG may identify vulnerabilities in IT systems that malicious cyber actors could exploit. USD(I&S) sponsored the DC3 advanced sensor program to detect and respond to adversary targeting of commercial critical infrastructure entities, including DIB contractors. USD(I&S) will continue to coordinate with interagency partners to develop policies and procedures for implementing DC3-monitored sensors. Voluntary implementation on DIB contractor networks will allow DC3 to aggregate and analyze collections from these sensors and disseminate threat information to targeted entities.

DOD STAKEHOLDER: USD(I&S) oversees classified threat intelligence sharing related to DIB cybersecurity activities, CI, and foreign ownership control or influence. USD(I&S) oversees the National Industrial Security Program policy and management through the DCSA and supports DIB cybersecurity activities related to classified information.

DC3 executes programs to analyze an organization's vulnerability to threat actors based on network architecture, software, and processes. It includes technical, process, and policy evaluations in a single, actionable framework. DC3 also conducts penetration testing, which includes network mapping, vulnerability scanning, phishing assessments, and web application testing.

Through the auspices of the DoD DIB CS program, NSA helps DIB customers find and fix issues before they become compromises by identifying DIB Internet-facing assets, then leveraging commercial scanning services to find vulnerabilities or misconfigurations on these networks. Each customer receives a tailored report with issues to remediate that is prioritized based on both severity of the vulnerability and whether it is being exploited.

Vulnerabilities in IT put at risk sensitive and proprietary information of the U.S. government and U.S. companies as well as that of allies and partners. To address this, the USG created the Vulnerabilities Equities Policy and Process (VEP)[22] for USG departments and agencies to balance equities and make determinations regarding the disclosure or restriction of newly discovered and not publicly known vulnerabilities in information systems and technologies. In alignment with the *National Security Strategy*'s call to "work in common cause with partners around issues of shared interest,"[23] the Department will coordinate and collaborate with allies and partners, to include at the interagency and state levels, to mitigate these risks.

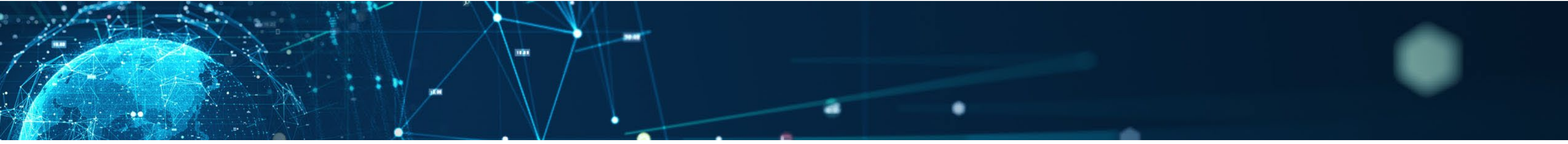
Objective 2.4 Recover from malicious cyber activity

Despite the application of the most robust cybersecurity posture available, the Department and the DIB must anticipate and prepare for recovery operations after a suspected malicious cyber activity has been detected, which may include the involvement of LE/CI authorities and capabilities from across the Department of Defense. Once a DIB contractor submits a cyber incident report, stakeholders within DoD execute activities to understand, assess, and mitigate the loss of CDI. Each stakeholder community plays a key role in implementing recommended mitigation actions to ensure DIB operations continue uninterrupted and federal information is protected. The Department will continue to develop and optimize these capabilities and ensure the broadest and most effective support to the DIB.

DOD STAKEHOLDER: Within USD(R&E), the Maintaining Technology Advantage Directorate leads DoD efforts to balance the promotion and protection of critical and enabling technologies throughout the technology development lifecycle. Critical to recovery assessment activities is the subordinate OSD DAMO, which provides oversight of all cyber incident damage assessment activities in the Department (e.g., OSD, Army, Navy, and Air Force). The DAMOs conduct impact assessments on the loss of CDI based on the unauthorized access and potential compromise of unclassified DIB information systems and networks. The DAMOs provide comprehensive operational, programmatic, technological, and manufacturing impact assessments that inform the DoD stakeholder communities of recommended mitigation actions.

[22] The USG created the VEP in accordance with paragraph (49) of National Security Policy Directive-54/Homeland Security Policy Directive-23, Cybersecurity Policy, and the Joint Plan for the Coordination and Application of Offensive Capabilities to Defend U.S. Information Systems.

[23] *National Security Strategy*, White House, October 2022, pg. 2, at https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.



Objective 2.5 Evaluate the effectiveness of cybersecurity regulations, policies, and requirements

The Department must continually evaluate its cybersecurity regulations and policies, such as DFARS 252.204–7012, as well as its programs, pilots, and cybersecurity services for how effectively these offerings meet the future challenges of a dynamic cyber threat landscape and contribute to a vibrant, innovative DIB. While implementing a more robust compliance regime, the Department will actively collaborate with the DIB to plan and execute pilots to test the efficacy of new and existing DIB cybersecurity capabilities, services, and processes. The DoD CIO recently released DoD Instruction 8530.03, *Cyber Incident Response,*[24] which reiterates DC3's responsibility for DIB cyber incident reporting and establishes a baseline dataset associated with cyber incident reporting across the Department. The alignment of reporting requirements supports future efforts to evaluate effectiveness of incident reporting and will be incorporated into a future revision of DoD Instruction 5205.13, *DIB Cybersecurity Activities*.[25]

The Department, in collaboration with the DIB, will seek to measure the effectiveness of cybersecurity requirements associated with programs, pilots, and services to inform subsequent efforts and iterative improvements. Within the OUSD(A&S), for example, the Cyber Warfare Directorate (CWD) will conduct pilots which focus on securing defense critical supply chains of prioritized weapon systems. As such, USD(A&S) is working with DoD stakeholders and DIB contractors to identify gaps in current cybersecurity-as-a-service (CSaaS) offerings and conduct pilots to improve the cybersecurity of the DIB. The CWD is also seeking to evaluate the cost-benefit of DIB cybersecurity efforts to address challenges incurred by DIB small businesses in implementing cybersecurity. The Department, in coordination with the DIB, will apply lessons learned from pilots to inform decisions and efforts which seek to improve support to small and medium-sized businesses in the progression toward cybersecurity maturity.

DOD STAKEHOLDER: Inside USD(A&S), the Office of Small Business Programs (OSBP) is the principal advisor to the Secretary of Defense on small business matters and assists small businesses with cybersecurity readiness assessments, threat and vulnerability information, and appropriate tool solutions to obtain and maintain cybersecurity hygiene and compliance. OSBP initiated Project Spectrum to provide cybersecurity education, increase cybersecurity awareness, and serve as a compliance resource for small businesses.

[24] DoDI 8530.03, *Cyber Incident Response*, DoD, August 9, 2023, at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853003p.PDF?ver=XPp9bgbmddCqR7gokbskWg%3D%3D.

[25] DoDI 5205.13, *Defense Industrial Base Cybersecurity Activities*, January 29, 2010, incorporating Change 2 August 21, 2019, at https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/520513p.pdf.

GOAL 3.
Preserve the resiliency of critical DIB capabilities in a cyber-contested environment

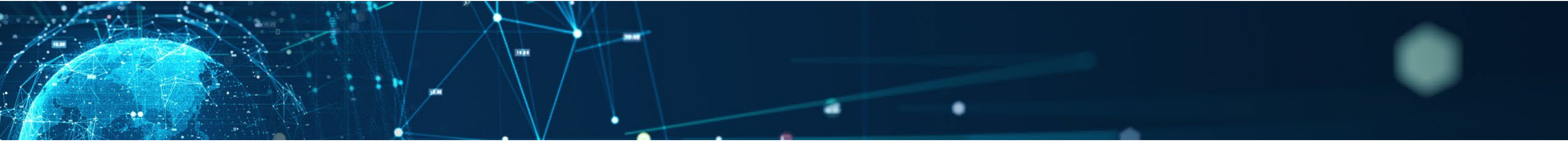
Recent global and geopolitical events have highlighted U.S. dependence on foreign and sole-source suppliers and signaled the need for increased attention to supply chain vulnerabilities and dependencies. Close coordination with sector-specific partners in a multi-tier cybersecurity ecosystem contributes to the development of requirements and best practices and provides early warning of bottlenecks in the supply chain of any critical system.

Objective 3.1 Prioritize the cyber resiliency of critical DIB production capabilities

The DIB is a vast attack surface for malicious cyber activity. Ensuring the continued integrity of DoD's most critical assets requires the Department to evaluate and subsequently prioritize those production capabilities that may be most vulnerable to disruption. The NDIS prioritizes resilient supply chains and the need for the DIB to be able to produce the products, services, and technologies at speed and scale. "The Department requires a resilient, healthy, diverse, dynamic, and secure supply chain to ensure the development and sustainment of capabilities critical to national security."[26] Segmentation of the tens of thousands of companies that compose the DIB is integral to ensuring that the limited resources of stakeholders can be focused on the most impactful protection activities. This segmentation requires continued collaboration across the Department, and across the USG through the construct of the DIB GCC, so that all stakeholder equities are adequately captured and all risks to critical production capabilities are accurately assessed. The DIB GCC is the counterpart to the private industry-led DIB Sector Coordinating Council (SCC). Together, the two councils work within the CIPAC to identify and share information on threats, assess and mitigate vulnerabilities, and monitor the security and resiliency of the DIB.

Figure 10: Representatives from The Boeing Company tour Portland Air National Guard Base (PANGB) on May 10th, 2022, Portland, OR. Boeing Representatives were visiting PANGB to learn more about the station in preparation for the rollout of the company's F-15EX Eagle II. Boeing is hoping to deliver the Eagle II to PANGB within the decade. U.S. Air National Guard photo by Staff Sgt. Alexander Frank.

[26] *National Defense Industrial Strategy 2024*, Department of Defense, pg. 6.



Objective 3.2 Establish in policy the priority focus on cybersecurity for critical suppliers and facilities

The Department continues to mature its policies on multi-tier supply chain cybersecurity risk. Coordination and integration of organizational policies and plans are needed to set clear and consistent guidelines on roles and responsibilities related to the cybersecurity of the DIB supply chain. As the SRMA for the DIB according to PPD-21, the Secretary of Defense designates a Principal Cyber Advisor as the coordinating authority for cybersecurity issues relating to the DIB. This role leads all DIB risk management activities for the Department, to include directing the focus of government-led protection efforts towards critical DIB capabilities and suppliers.

DOD STAKEHOLDER: USD(P) performs SRMA functions and serves as the overall risk manager for the DIB as executed by the Office of Defense Continuity and Mission Assurance (DC&MA). DC&MA serves as the Department's external facing interface, especially with DHS, the DIB SCC, and other critical infrastructure sectors. DC&MA convenes and coordinates with stakeholders and develops whole-of-Department strategies for addressing all threats to the DIB.

Figure 11: From the factory floor … Lockheed Martin employees work on the F-35 Lightning II Joint Strike Fighter production line in Fort Worth, TX. Defense Contract Management Agency LM Fort Worth Keystones support the vital Department of Defense mission of administering Joint Strike Fighter contracts.

GOAL 4.
Improve cybersecurity collaboration with the DIB

Strengthening cybersecurity collaboration with the DIB is a strategic priority for the Department. The Department in coordination with the federal government must streamline and evaluate the communication pathways used for routine and critical cybersecurity awareness. Consistent communication also contributes to the practical adoption of cybersecurity requirements. Collaboration with the DIB should include pilot programs in cybersecurity, war-gaming, routine engagement with industry working groups, cybersecurity training pathways, and cross-cutting education and awareness campaigns provided by multiple federal agencies.

Given the diversity and scale of the DIB, different businesses may need or benefit from different services, support, and information such as training and education or a range of cybersecurity services. The Department will invest in further defining subsectors of the DIB and tailoring programs for these DIB subsectors. Ultimately, the Department, in collaboration with the DIB, seeks to ensure that the DIB is prepared to operate securely in the cyberspace domain without introducing undue costs or burdens.

Objective 4.1 Leverage collaboration with commercial Internet, cloud, and cybersecurity service providers to enhance DIB cyber threat awareness

The NSA CCC maintains bidirectional cooperatives across multiple core technology sectors, including, but not limited to cloud service providers, endpoint protection, Internet service providers, threat intelligence firms, and others. NSA analysts work daily with industry and interagency partners to detect, mitigate, and eradicate malicious cyber activity. As malicious cyber activity is identified, the CCC will inform the impacted entities of the activity and work with them until it has been eradicated. It will also share this information with the DIB, empowering it to harden billions of endpoints across the globe against emerging sophisticated cyber threats, with ripple effects across all U.S. critical infrastructure, its allies, industry, and individual consumers alike.

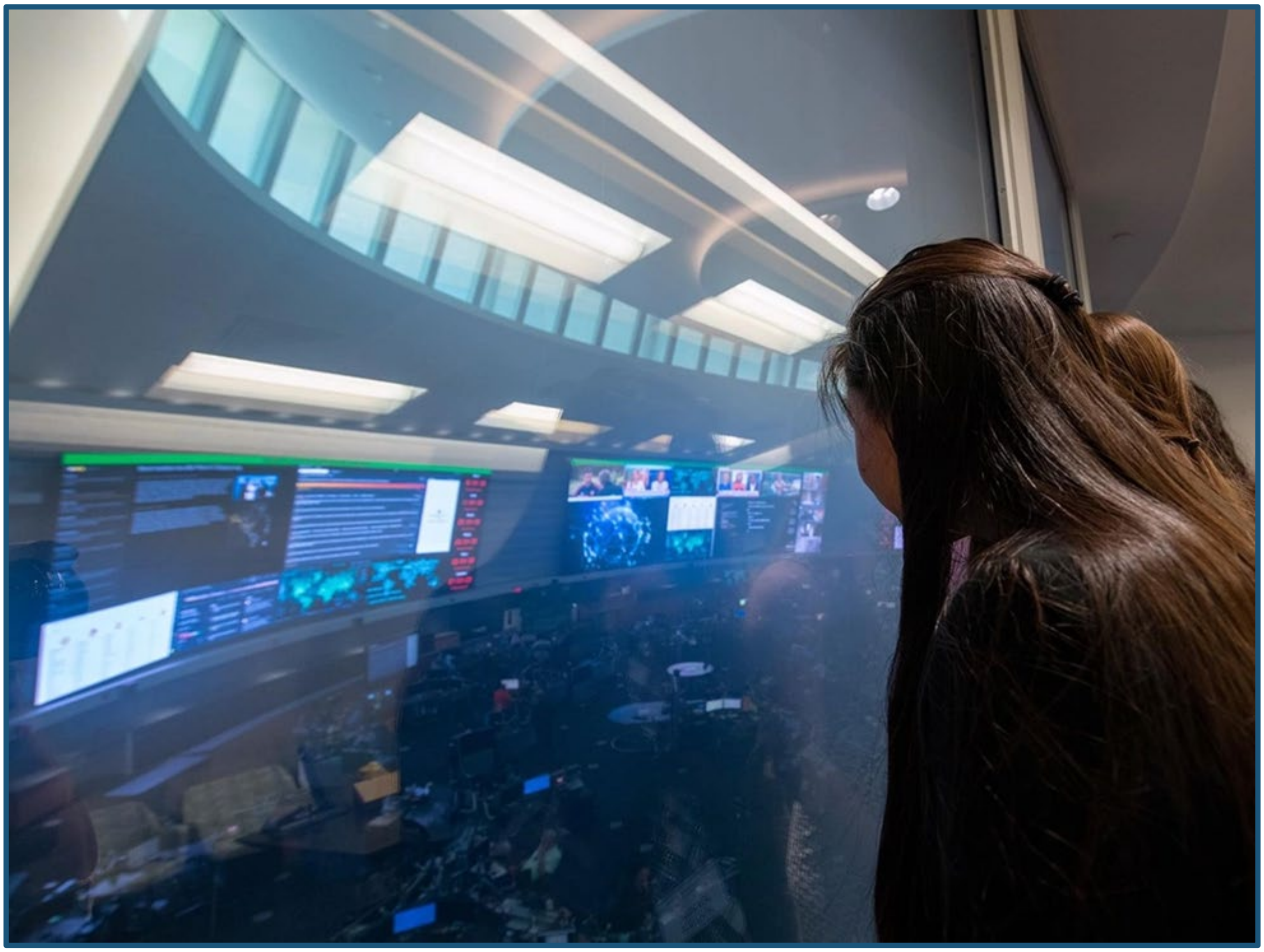
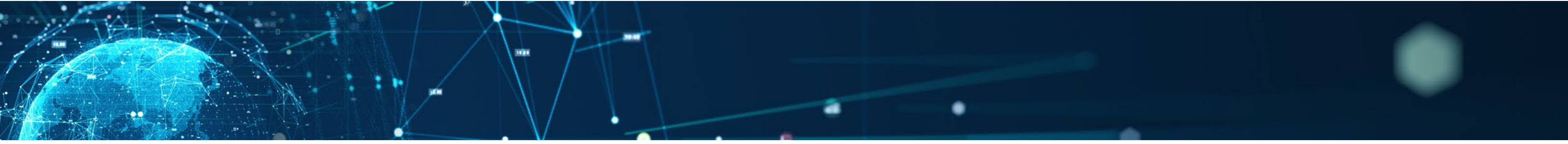


Figure 12: Illuminating the Future of Cybersecurity: Students tour NSA's state-of-the-art Integrated Cyber Center/Joint Operations Center at NSA Washington East Campus.



Objective 4.2 Work with the DIB SCC to improve communication and collaboration with the DIB

The Department seeks engagement with the DIB SCC to facilitate expanded sharing and analysis of aggregated and anonymized cyber incident trends to advance DoD's understanding of the cybersecurity posture of the DIB. This information will be used to identify approaches for improved mitigation efforts and greatly improve the effectiveness of the DoD DIB Cybersecurity Program and the cybersecurity posture of the DIB.

To further support the DIB SCC's role in identifying issues and potential solutions of mutual interest to the DIB and the Department of Defense, as appropriate the DoD CIO will invite members from the DIB SCC Executive Committee and designated staff from the Information/Cybersecurity Standing Committee to serve advisory roles in the DoD DIB Cybersecurity Program. Chartered to enable sharing of information and timely notification related to malicious cyber activity, the DIB GCC will coordinate with the DIB SCC Information/Cybersecurity Standing Committee to catalog obstacles to information sharing with the DIB and produce proposals for the mitigation of cybersecurity risk to sensitive data and missions.

Objective 4.3 Improve bidirectional communication with the DIB and expand public-private cybersecurity collaboration

Paramount to this strategy is improving communication with the DIB. The Department is committed to providing timely, relevant, and actionable threat intelligence to DIB contractors and will continue to advance efforts to share information both through human-to-human and machine-to-machine exchanges to deepen the connection between its cyber incident reporting and vulnerability management programs. Operational collaboration must be bolstered by appropriate technology solutions to share information and support prioritization of defensive efforts. By strengthening the connection with industry, researchers and the Department may reduce the time required to discover previously unknown vulnerabilities to share broadly within the community.

Recognizing that cyber incidents are inevitable, the Department will also engage with industry on ways to bolster capabilities to respond and recover from malicious cyber activities. The Department will devote resources to develop cyber incident scenarios and validate cyber incident response playbooks. DC3, DCSA, NSA, and USCYBERCOM all actively contribute to these efforts, but no single agency can defend the Nation on its own. The Department will continue to collaborate with domestic partners across the federal government, sector-focused information sharing and analysis centers (ISACs), and SLTT to share best practices and expertise.

A View from the Nation's Cyber Commanders
Speakers:
Lieutenant General Maria B. Barrett, Commanding General, United States Army Cyber
Vice Admiral Craig A. "Clap" Clapperton, Commander, United States Fleet Cyber Com
Space/United States TENTH Fleet
Major General William J. Hartman, Commander, Cyber National Mission Force
Major General Joseph "Jay" Matos, Deputy Commander, Marine Corps Forces Cybersp
Command/Joint Forces Headquarters-Cyber
Lieutenant General Robert Skinner, Director, Defense Information Systems Agency
and Commander, Joint Force Headquarters-DOD Information Networks
Rear Admiral John C. Vann, Commander, Coast Guard Cyber Command
MG Matthew D. Dinmore, Air National Guard Assistant to the Commander,
16th Air Force (Air Forces Cyber)
Moderator:
paloalto NETWORKS
JSAC
REGIMENT OF ARTILLERY
WE FIGHT

Figure 13: The U.S. Military Academy, on behalf of Palo Alto Networks, Inc., hosted the 2023 Joint Service Academy Cybersecurity Summit (JSAC) on April 4-5 at Crest Hall in Eisenhower Hall. Founded in 2015, JSAC brings together senior cyber experts and leaders from across industry, military, and government to discuss issues of the day, what has gone right and what has gone wrong in cybersecurity in recent years and the way forward in the cyber world.

The DoD DIB Cybersecurity Program is a public-private cybersecurity cooperative with over one thousand DIB companies participating in the voluntary program and membership is expected to increase in 2024 with a revision to the eligibility criteria.[27] Once Program participants' DIBNet accounts are fully activated, they can engage with the Program and DC3 to receive cyber threat information and participate in program-related engagements, such as working groups and DIBNet forums.

NSA coordinates engagements with the private sector to provide cybersecurity assistance to DIB entities and associated service providers. NSA's CCC facilitates threat information-sharing between intelligence and industry members to ensure DIB and service provider systems are secure. The NSA also provides cybersecurity services and assistance to help DIB contractors detect system vulnerabilities and counter malicious cyber activity.

Through DoD's public-private DoD DIB Cybersecurity Program, the NSA CCC, and the DC3 DCISE, the Department will provide CSaaS offerings (see Appendix III) to eligible DIB contractors in a scalable and cost-effective manner. These offerings encompass training and awareness as well as access to commercial cybersecurity services which perform attack surface management, vulnerability scanning, threat detection and blocking, and various other capabilities.

[27] The pending revision to Part 236 of Title 32 CFR allows a broader community of defense contractors to benefit from bilateral information sharing with DoD, as all defense contractors who are subject to mandatory cyber incident reporting are now able to participate in the DoD DIB Cybersecurity Program.

The Department will centralize information about DIB cybersecurity policies, regulations, and government/industry resources, including a catalog of relevant CSaaS capabilities, information-sharing programs, resourcing programs, cyber workforce qualification requirements, and training/education activities; as well as optimize the searchability of, authoritativeness of, and the consumer experience for this information. Various offices in the Department produce, maintain, and facilitate programs and services to help DIB contractors bolster cybersecurity. While these services provide immense value to the DIB, access to these resources is managed by the offices providing them and limited by different authorities. Increased socialization of these efforts across stakeholder offices within the Department and the DIB will increase effectiveness by way of improved coordination. To ensure that these resources are close-at-hand to DIB stakeholders, the DoD CISO will create and maintain a comprehensive list detailing these offerings. This product will be made publicly available through multiple means, including through the unclassified web-based capabilities already leveraged by the DIB community and the DoD CIO library.

One such resource available to the DIB is the NIST CSF. NIST is currently working on releasing CSF 2.0, which will provide technical assistance on alignment of regulations with international standards and the NIST CSF. The Department can advance cybersecurity interests by sharing DIB sector-specific expertise and contributing to coordinating policy.

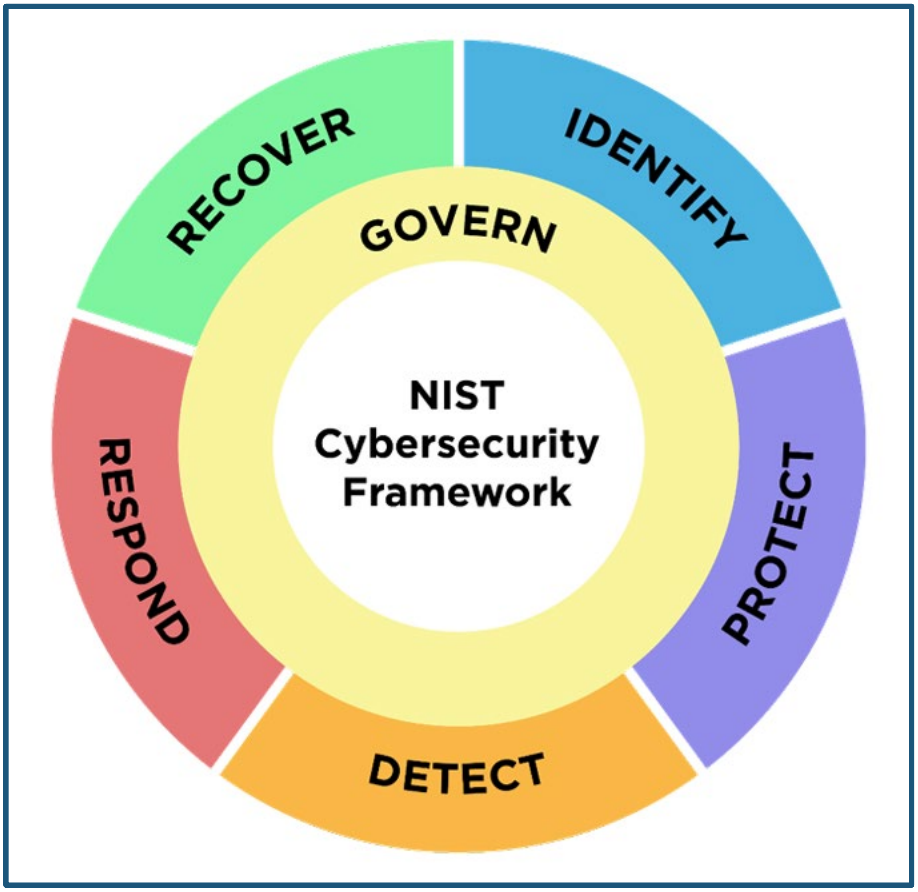
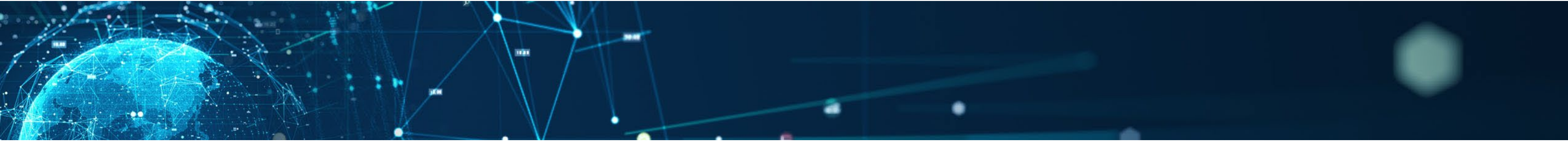


Figure 14: The NIST Cybersecurity Framework 2.0 Core

.



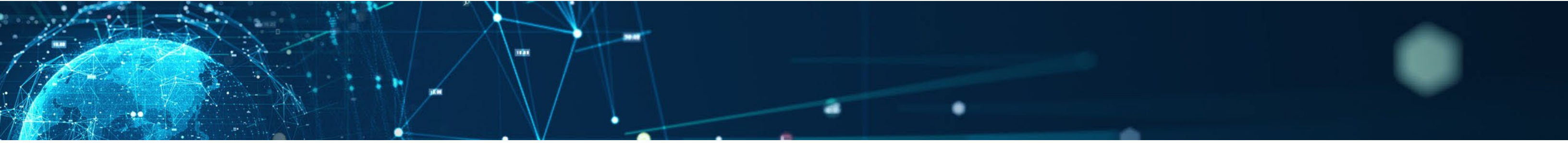
CONCLUSION

Achieving the objectives laid out in this strategy requires coordination of effort across all DoD entities in alignment with the NDS, the *National Cybersecurity Strategy*, and the *DoD Cyber Strategy*. The Department plays a key role in educating, measuring, and driving improvements in all matters related to DIB cybersecurity. Protecting critical defense information and preserving competitive advantage requires the Department to invest in measures to bolster DIB cybersecurity, while being cognizant of the risk associated with burdensome compliance costs that discourage competition. Successful implementation of the *DoD DIB Cybersecurity Strategy* requires engagement external to the Department and the Department to set an example of cyber resiliency.

The Department must pursue the goals outlined above as an enterprise and operate in lockstep with the whole-of-government effort to better secure cyberspace. While this is an enormous task, the Department is driving progress across multiple fronts. Since 2008, DoD CIO's voluntary DoD DIB Cybersecurity Program has shared cyber threat information, including mitigation strategies and threat indicators, with cleared industry, helping both industry and government to better understand cyber threats and prevent attacks. Since publishing DFARS 252.204-7012 in 2013, the Department has required Defense contractors to safeguard sensitive defense information by establishing baseline cybersecurity requirements and cyber incident reporting requirements. In 2019, the OSBP launched Project Spectrum followed by NSA launching the CCC in recognition of the widely differing cyber capabilities of companies that interact with the Department and to focus resources to meet companies at their level.

Supporting the national priority of integrated deterrence means preparing for crisis and conflict while campaigning in competition across the full gamut of cyber operations. It also means building the strategic partnerships that enable the defense of U.S. systems and networks beyond the DODIN and the DIB. The Department will continue to seek technical expertise from NSA, DC3, and USCYBERCOM to understand trends and influence policies to continuously improve security and resilience. Over the past several years, DIB contractors have been working to improve cyber resilience, comply with existing security requirements, and better understand the evolving threat. This represents a huge shift in cyber threat awareness and emphasis on DIB resources committed to securing unclassified DIB networks.

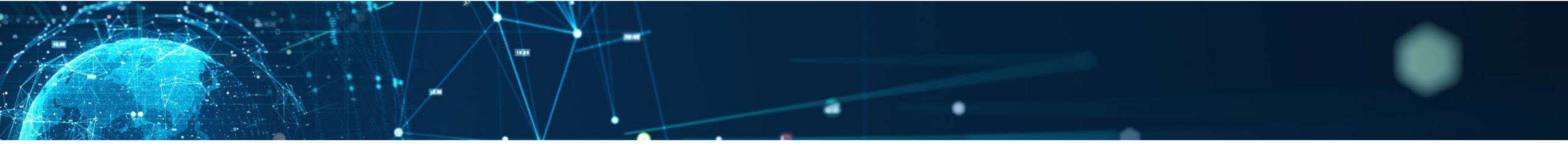
This Strategy lays out the vision for the Department to further coordinate and execute resources in a collaborative manner with the DIB to effect change to the cybersecurity of our Nation's most critical defense suppliers and producers. Our adversaries will not rest in their campaigns to seek information about U.S. capabilities; look for shortcuts to advanced technology; and counter, kill, or clone our warfighting capabilities. The Department of Defense, in coordination with the DIB, must remain resilient against these attacks and succeed through teamwork while defending the Nation.



APPENDIX I – ACRONYMS AND ABREVIATIONS

ACRONYM	**MEANING**
AET	Adversary Emulation Tests
APT	Advanced Persistent Threat
CADO-IS	Collect, Analyze, Disseminate, and Operationalize - Integrated Solution
CCC	Cybersecurity Collaboration Center
CDI	Covered Defense Information
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CIPAC	Critical Infrastructure Partnership Council
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CMMC	Cybersecurity Maturity Model Certification
CRA	Cyber Resilience Assessment
CSaaS	Cybersecurity-as-a-Service
CSF	Cybersecurity Framework
CUI	Controlled Unclassified Information
CWD	Cyber Warfare Directorate
DAMO	Damage Assessment Management Office
DC&MA	Defense Continuity and Mission Assurance
DC3	DoD Cyber Crime Center
DCISE	DoD-DIB Collaborative Information Sharing Environment
DCSA	Defense Counterintelligence and Security Agency
DFARS	Defense Federal Acquisition Regulation Supplement
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DIBCAC	DIB Cybersecurity Assessment Center
DoD	Department of Defense
DODIN	Department of Defense Information Networks
DSD	Deputy Secretary of Defense
EO	Executive Order
ESG	Executive Steering Group
FAR	Federal Acquisition Regulation
FY	Fiscal Year
GCC	Government Coordinating Council
ISAC	Information Sharing and Analysis Center
IT	Information Technology

ACRONYM	MEANING
LE/CI	Law Enforcement/Counterintelligence
NDAA	National Defense Authorization Act
NDIS	National Defense Industrial Strategy
NDS	National Defense Strategy
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OSBP	Office of Small Business Programs
PPD	Presidential Policy Directive
SCC	Sector Coordinating Council
SLTT	State, Local, Tribal, and Territorial
SP	Special Publication
SRMA	Sector Risk Management Agency
SSP	Sector-Specific Plan
USCYBERCOM	United States Cyber Command
USD(A&S)	Under Secretary of Defense for Acquisition & Sustainment
USD(I&S)	Under Secretary of Defense for Intelligence & Security
USD(P)	Under Secretary of Defense for Policy
USD(R&E)	Under Secretary of Defense for Research & Engineering
USG	United States Government
VEP	Vulnerabilities Equities Policy and Process



APPENDIX II – U.S. DIB SECTOR

As one of the sixteen critical infrastructure sectors identified in PPD-21, *Critical Infrastructure Security and Resilience*, the DIB is best defined as the set of domestic and foreign companies or organizations—at all levels—that perform research and development, design, production, delivery, and maintenance of DoD systems, subsystems, and components or parts, as well as those who provide software and other critical services to meet U.S. defense requirements. PPD-21 defines "infrastructure" as a collection of assets, systems, networks, entities, critical services, or organizations and sets forth sixteen sectors. The sectors, while grouped by uniqueness, have strong areas of overlap. The 2021 NDAA Section 9002(b) Report calls for regular reviews of critical infrastructure sectors and for all SRMAs, coordinating through the Federal Senior Leadership Council, to update SSPs outlining specific authorities and capabilities, objectives, priorities, adding a five-year roadmap outlining key activities to be implemented in carrying out the responsibilities under Section 665d of Title 6, United States Code.

The DIB Sector produces highly specialized products and parts for which special attention, risk controls, and investment is needed. Although it maintains strong interdependencies with several other critical infrastructure sectors, the DIB warrants its own sector designation since it shares a united purpose in production and is governed by laws related specifically to DIB entities. The relationship between DIB and Critical Manufacturing is linked through production, which is further connected to the Chemical sector as many compounds and chemicals are integral to manufacturing processes. In addition, chemicals are required for defense-related explosives and weapons systems. The IT sector is a functions-based critical infrastructure sector that comprises not only physical assets, but also virtual systems and networks that enable key capabilities and services in both the public and private sectors. The IT sector includes hardware manufacturers, software developers, service providers as well as the Internet as a key resource. The DIB sector relies on the IT sector for routine business, but this sector has also emerged as a major threat vector in addition to being an enabler of Defense equities.

The Transportation Systems infrastructure has a common purpose of providing efficient, safe, and secure freedom of movement for people and commerce across the Nation's transportation systems. The infrastructure in this sector is diverse and distinct, and is segmented into subsector modals: Aviation, Maritime, Freight Rail, Highway and Motor Carrier, Pipeline, Postal and Shipping, and Mass Transit. Unlike most critical infrastructure sectors that feature one overall SCC, this sector has a SCC for each of the respective Transportation System subsector modals. There is not one all-encompassing ISAC or Information Sharing and Analysis Organization for this critical infrastructure sector, instead there are a variety of organizations covering the various subsector modals (e.g., Surface Transportation ISAC, Aviation ISAC). The DIB sector has a heavy reliance on transportation for movement of goods or people.

Section 1715 of the NDAA for FY 2021 amended the Homeland Security Act of 2002 by adding a Joint Cyber Planning Office. This amendment directed that each SRMA shall utilize its specialized expertise to perform several responsibilities related to the designated critical infrastructure sector or subsector. These responsibilities include assessing sector risk, maintaining situational awareness, supporting sector risk management, executing sector coordination, conducting bi-directional information sharing regarding physical and cybersecurity threats, supporting incident management, and contributing to emergency preparedness efforts with industry and at the SLTT levels. SRMAs will coordinate directly with state and local agencies relevant to each designated sector (e.g., public utility commissions). The USD(P) has the responsibility for DoD tasks associated with PPD-21 and further coordinates with DoD CIO for matters specific to DIB cybersecurity.

DOD and Defense Industrial Base Sector Risk Management Agency

What is Critical Infrastructure?

The nation's critical infrastructure provides the essential services that underpin American society.

Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure that are vital to public confidence and the nation's safety, prosperity, and well-being.

16 Critical Infrastructure "Sectors"

Chemical	Commercial Facilities	Communications	Critical Manufacturing
Dams	Defense Industrial Base	Emergency	Energy
Financial Services	Goods and Agriculture	Government Facilities	Water and Wastewater
Information Technology	Nuclear Reactors, Materials, and Waste	Transportation	Healthcare and Public Health

What is the Defense Industrial Base?

The Defense Industrial Base (DIB) is the set of U.S. and allied companies or organizations – at all levels – that perform research and development, design, production, delivery, and maintenance of DoD systems, subsystems, and components or parts, as well as those who provide software and other critical services to meet U.S. defense requirements. It is one of 16 critical infrastructure sectors the U.S. has a dedicated effort to support and manage risk, leveraging public-private partnership with industry.

- The DIB includes approximately 300,000 defense companies and their suppliers throughout the defense and private sectors.

DIB Public-Private Partnership

- The Strategic Priority: Ensure generation, reliability, and preservation of U.S. warfighting capabilities
- Threat: Adversaries seek to clone, counter, or destroy U.S. military capabilities, using economic, financial, cyber, intelligence, and other means.
- Integrated Deterrence: Protect common interests, through public-private partnerships
- Structure: Government Coordinating Council, Sector Coordinating Council, and joint Critical Infrastructure Partnership Advisory Council*.
- Approach: OUSD/Policy as DIB SRMA convenes and coordinates efforts; DoD components shape and execute efforts within their mission areas.

*The Homeland Security Act of 2002 (the "Act"), 6 U.S.C. § 101 et. seq., including sections 871(a) and 2202 of the Act, 6 U.S.C. §§ 451(a), 652, enables DHS to exempt CIPAC meetings from The Federal Advisory Committee Act (FACA), Public Law 42-463.)

DIB SRMA Lines of Effort (LOE) & Stakeholders

LOE 1 Convene & Coordinate

Advance Whole of Government Effort

Align Vision, Resources, and Organization

Break Down Barriers to Government & Industry Cooperation

LOE 2 Share Information

Ensure Bidirectional Exchange on Threats

Improve info access, flow, timeliness, and relevance

LOE 3 Assess Risks

Identify Critical Facilities, Programs, Technologies, Materials
-----
Assess Threats & Vulnerabilities

Identify Choke Points

LOE 4 Manage Risks

Ensure Critical Facilities Secure Against All Threats

Spur Efforts to Manage Risks to DIB + other Critical Infrastructure Sectors

LOE 5 Prepare for Emergencies

Advance Resilience & Security

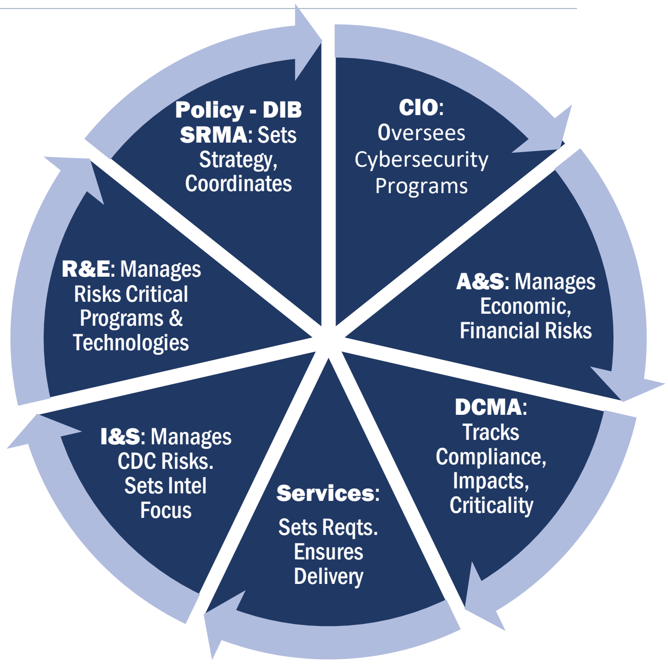
Ensure Communication

LOE 6 Incidence Response

Track Critical Facilities

Report on Impacts

Mitigate



Policy - DIB SRMA: Sets Strategy, Coordinates

CIO: Oversees Cybersecurity Programs

A&S: Manages Economic, Financial Risks

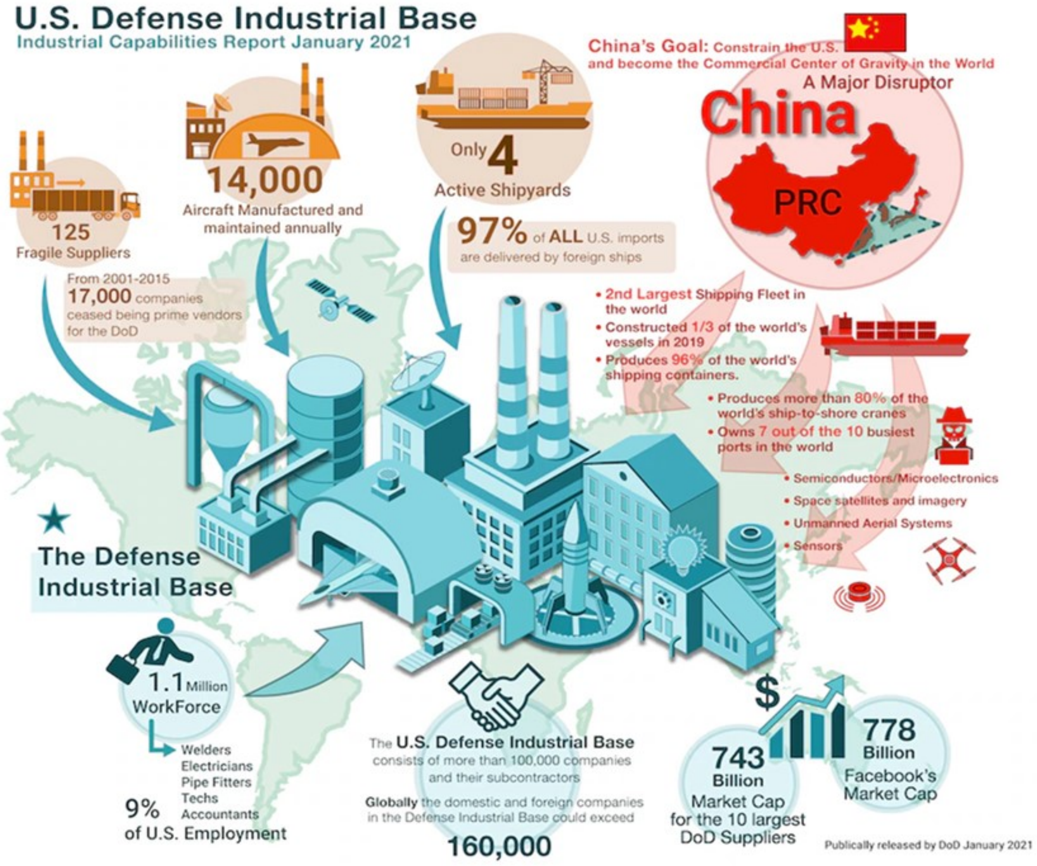
DCMA: Tracks Compliance, Impacts, Criticality

Services: Sets Reqts. Ensures Delivery

I&S: Manages CDC Risks. Sets Intel Focus

R&E: Manages Risks Critical Programs & Technologies

*As the SRMA for the DIB, DoD has several legislative responsibilities, that it accomplishes through six LOEs. This is achieved in collaboration with offices across DoD.



U.S. Defense Industrial Base

Industrial Capabilities Report January 2021

125
Fragile Suppliers

From 2001-2015
17,000 companies
ceased being prime vendors
for the DoD

14,000
Aircraft Manufactured and
maintained annually

Only 4
Active Shipyards

97% of ALL U.S. imports
are delivered by foreign ships

China's Goal: Constrain the U.S.
and become the Commercial Center of Gravity in the World

A Major Disruptor

China

PRC

- 2nd Largest Shipping Fleet in the world
- Constructed 1/3 of the world's vessels in 2019
- Produces 96% of the world's shipping containers.

- Produces more than 80% of the world's ship-to-shore cranes
- Owns 7 out of the 10 busiest ports in the world

- Semiconductors/Microelectronics
- Space satellites and imagery
- Unmanned Aerial Systems
- Sensors

The Defense
Industrial Base

1.1 Million
WorkForce

Welders
Electricians
Pipe Fitters
Techs
Accountants

9%
of U.S. Employment

The U.S. Defense Industrial Base
consists of more than 100,000 companies
and their subcontractors

Globally the domestic and foreign companies
in the Defense Industrial Base could exceed
160,000

743
Billion
Market Cap
for the 10 largest
DoD Suppliers

778
Billion
Facebook's
Market Cap

Publically released by DoD January 2021

Managing DIB risk is a critical aspect of competition and integrated deterrence vis-à-vis the People's Republic of China (PRC) in support of National Defense Strategy (NDS) objectives. The PRC is conducting a focused campaign to undermine the nation's operational effectiveness and obtain information on sensitive DIB acquisition programs in technology, leveraging multiple vectors as shown in this slide from the January 2021 Industrial Capabilities Report.

Threats and Vulnerabilities

The DIB sector faces multiple challenges including climate impacts, intellectual property theft, predatory financial practices, insider threats, cyber, and other nefarious

practices that erode the nation's domestic capabilities and ultimately affect the DoD's ability to fight in large scale wars with peer competitors. Particular incidents of note include:

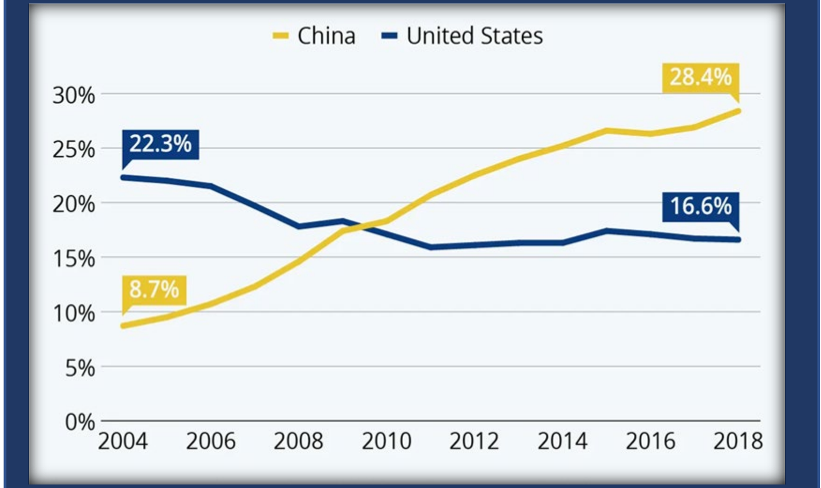
- Chinese investments in U.S. industry and agriculture almost certainly provide the Chinese Communist Party (CCP) with undue leverage over U.S. supply chains and access to sensitive information critical to US national security.
    - According to US Department of Agriculture (USDA) reports, Chinese investors' holdings of US agricultural land surged from 13,720 acres in 2010 to 352,140 acres in 2020.
- The annual cost to the U.S. economy of counterfeit goods, pirated software, and theft of trade secrets is $225–$600 billion.

Questions?

Defense Industrial Base SRMA Support –
DIBSRMASupport@mail.mil

China's Rise to Manufacturing Dominance

Chinese and U.S. share of global manufacturing output*



To date, China has a near monopoly on rare-earth metals that are critical for manufacturing various missiles and munitions. China also dominates the advanced battery supply chain across the globe, such as lithium hydroxide, cells, electrolyte, lithium carbonate, anodes, and cathodes.

** Output measured on a value-added basis in current U.S. dollars*
Source: United Nations Statistics Division

APPENDIX III

U.S. Department *of* Defense

CLEARED
For Open Publication
Jun 27, 2023
4
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Department of Defense (DoD) Defense Industrial Base (DIB) **Cybersecurity-as-a-Service (CSaaS)** Services and Support

The DoD recognizes the need to help DIB organizations improve their cybersecurity posture and operational resilience and to help the DIB protect DoD information that resides on and transits DIB information systems.

What is this?

Free cybersecurity services and information provided by the DoD to DIB organizations

Who is this for?

All members of the DIB

How?

A variety of services are available based on your specific needs. Visit the websites below for information about cybersecurity training, services, and products. You may also contact the DIB CS PMO at **OSD.DIBCSIA@mail.mil** to request additional details about these services.

DC3/DOD DEFENSE INDUSTRIAL BASE COLLABORATIVE INFORMATION SHARING ENVIRONMENT (DCISE)

Eligibility: The DIB CS Program is open to cleared defense contractors. The DoD has proposed changes to the eligibility requirements outlined in 32 CFR part 236 that will expand the program to contractors that own or operate a covered contractor information system.

DCISE[3]

CATEGORIES

- network traffic monitoring
- threat detection and blocking

DCISE has partnered with a service provider to offer real-time monitoring of your organization’s network traffic, threat detection, and alerts as well as the option to block malicious traffic.

This service includes real-time network traffic monitoring for malicious sources and destinations and shares data anonymously at no cost. Malicious traffic is alerted on and, if desired, blocked. The service protects against DDOS and DNS attacks.

https://www.dc3.mil or email **DC3.Information@us.af.mil**

CYBER RESILIENCE ANALYSIS (CRA)

CATEGORY

- cybersecurity program evaluation

This program offers a structured review of an organization’s cybersecurity posture with the goal of understanding cybersecurity capabilities and operational resilience and improving the ability to manage risk to critical services and assets.

A structured survey conducted either in a DC3-facilitated session or as a self-assessment produces a report with suggested actions aligned with the 10 security domains that map to the NIST SP 800-171 requirements to protect CUI and the NIST Cybersecurity Framework.

https://www.dc3.mil or email **DC3.Information@us.af.mil**

ADVERSARY EMULATION (AE)

CATEGORIES

- network mapping
- vulnerability scanning
- phishing assessments

This program analyzes an organization’s vulnerability to threat actors based on network architecture, software, and processes. It includes technical, process, and policy evaluations in a single, actionable framework.

AE may include penetration testing, network mapping, vulnerability scanning, phishing assessments, and web application testing.

https://www.dc3.mil or email **DC3.Information@us.af.mil**

DoD DIB CSaaS

NATIONAL SECURITY AGENCY (NSA) CYBERSECURITY COLLABORATION CENTER

Eligibility: Any company (prime or sub) with a DoD contract and access to non-public DoD information

PROTECTIVE DOMAIN NAME SYSTEM (PDNS)

CATEGORIES

- network traffic monitoring
- threat detection and blocking

The NSA's PDNS service combines commercial cyber threat feeds with the NSA's unique insights to filter external DNS queries and block known malicious or suspicious website traffic, mitigating nation-state malware, spearphishing, botnets, and more.

https://www.nsa.gov/CCC or **DIB_Defense@cyber.nsa.gov**

ATTACK SURFACE MANAGEMENT

CATEGORIES

- asset discovery
- vulnerability scanning

This service helps DIB customers find and fix issues before they become compromises by identifying DIB internet-facing assets, then leveraging commercial scanning services to find vulnerabilities or misconfigurations on these networks. Each customer receives a tailored report with issues to remediate, prioritized based on both severity of the vulnerability and whether or not it is being exploited.

https://www.nsa.gov/ccc or **DIB_Defense@cyber.nsa.gov**

PROJECT SPECTRUM

CATEGORIES

- awareness
- training
- tools
- services (both free and paid)

Sponsored by the DoD Office of Small Business Programs (OSBP), Project Spectrum offers a wide variety of services, including cybersecurity information, resources, tools, and training. Their mission is to improve cybersecurity readiness, resiliency, and compliance for small and medium-sized businesses and the federal manufacturing supply chain.

Project Spectrum includes information about security, risk, and compliance assessments, readiness checks, training, reviews of tools, current research, and policy. Project Spectrum provides information about U.S. Government and commercial services and tools, both free and fee based.

https://www.projectspectrum.io/#/

BLUE CYBER INITIATIVE

CATEGORIES

- awareness
- training

The Department of the Navy CISO's Blue Cyber Education Series for Small Businesses provides free and open-to-the-public cybersecurity information and support.

Participate in daily, weekly, and monthly cybersecurity online help sessions and webinars. Learn about state and federal resources and collaborate across the federal, academic, and national small business ecosystem. Explore links to other DoD-sponsored Small Business Innovation Research cybersecurity programs.

https://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/

DEPARTMENT OF DEFE
CHIEF INFORMATION OFF

DIGITAL
MODERNIZATION
CYBER
CLOUD
WARFIGHTER
C3
INTEGRATED DETERRENCE
BUILDING ENDURING ADVANTAGES
CAMPAIGNING