# FY2025-2026 CISA International Strategic Plan

Publication: October 2024
Cybersecurity and Infrastructure Security Agency

# Table of Contents

## EXECUTIVE SUMMARY

In today's interdependent and interconnected world, the protection and security of our cyber and physical infrastructure requires the concerted efforts of public and private partners around the globe. The Cybersecurity and Infrastructure Security Agency (CISA) is a globally recognized leader in shaping and implementing proactive approaches to reduce risk and increase the resilience of critical infrastructure on which the United States (U.S.) and its partners depend.

To effectively marshal its resources and guide operations, CISA issued the 2023-2025 CISA Strategic Plan, the agency's first comprehensive strategic plan since CISA's establishment in 2018. In recognition of the reality that today's threats do not respect borders, CISA developed this CISA 2025-2026 International Strategic Plan as a complementary guide for CISA's international activities and outcomes.

This CISA 2025-2026 International Strategic Plan acknowledges that the risks we face are complex and geographically dispersed, and that we cannot achieve our objectives in a vacuum. It is imperative that we expand visibility into internationally shared systemic risks. The maturity and security practices of global owners and operators of both cyber and physical infrastructure, technology, supply chains, and systems vary widely. Sharing timely, relevant, and accurate threat information and risk reduction advice with international partners provides the foundation for a more secure cyber-physical environment for all of us.

The CISA 2025-2026 International Strategic Plan goals are to:

1. Bolster the Resilience of Foreign Infrastructure on Which the U.S. Depends.
2. Strengthen Integrated Cyber Defense.
3. Unify Agency Coordination of International Activities.

Through the goals and objectives outlined in this CISA 2025-2026 International Strategic Plan – in coordination with the Department of Homeland Security (DHS), the Department of State, and partners across the interagency, and in accordance with U.S. national security, economic, and foreign policy priorities – CISA will assess and prioritize critical infrastructure dependencies and partner with foreign entities to advance CISA's homeland security mission.

# 1. OUR MISSION

Our vision is secure and resilient infrastructure for the American people. Our mission is to lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

**Strategic Intent:** The CISA 2025–2026 International Strategic Plan will focus and guide the agency's international efforts over the 2025–2026 period. It highlights the agency's commitment to reducing risk to the globally interconnected and interdependent cyber and physical infrastructure that Americans rely on every day. Our aim is to shape the international environment to reduce risk to critical dependencies and set conditions for success in cooperation, competition, and conflict. The CISA 2025-2026 International Strategic Plan lays out three goals CISA must achieve to address the ever-changing and dynamic challenges facing America and our international partners. The first two goals focus on "what" the agency will work on in the international environment to achieve our "why" – 1) to reduce risk to and build resilience of foreign assets, systems, and networks that impact U.S. critical infrastructure, 2) understand shared global threats to critical infrastructure, and 3) support collective defense. The third goal focuses internally to promote unified action, working as One CISA to conduct international activities.

**Strategic Approach:** The approach laid out in this CISA 2025–2026 International Strategic Plan aligns with guidance set forth in the National Security Strategy, National Cybersecurity Strategy, U.S. International Cyberspace and Digital Policy Strategy, CISA Strategic Plan 2023–2025, CISA Stakeholder Engagement Strategic Plan FY2023-2025, and CISA Cybersecurity Strategic Plan 2024–2026, as well as the identified priorities of the Secretary of Homeland Security. The CISA 2025-2026 International Strategic Plan and the U.S. International Cyberspace and Digital Policy Strategy firmly align to bolster and broaden international alliances to mature cyber defense efforts, both domestically and internationally. This involves fostering collaborative relationships with global partners; sharing expertise, technical resources, and best practices; and collectively fortifying cyber resilience to address emerging threats in an interconnected world. Our strategic approach will not only advance the resilience of critical infrastructure dependencies at home and abroad, but it will also ensure a long-term commitment in strengthening international partnerships that are essential for CISA's mission success. As part of coordinated U.S. government efforts, CISA will proactively engage and support international partners to assess, influence, and assist with reducing risk and strengthen the security and resilience of foreign assets, systems, and networks on which our nation's critical infrastructure depends. As threats evolve across the spectrum of competition with state and non-state actors, no single organization or entity has all the answers for how to address cyber and physical threats to critical infrastructure. Therefore, CISA will prioritize operational collaboration and international activities to achieve mutual interests and goals with our partners. This plan centralizes CISA's focus and coordination on goals and objectives that increase homeland and national security. More importantly, it positions CISA to support the internal coordination of international activities through the execution of annual planning cycles. This CISA 2025-2026 International Strategic Plan seeks to streamline or eliminate overlapping and redundant systems to synchronize complex international issues that cut across our agency.

Overall, our aim is to build, strengthen, and sustain international relationships to:

1. Advance homeland and national security objectives.
2. Prevent incidents and increase resilience of physical and cyber critical infrastructure at home and abroad.
3. Increase awareness to detect, deter, and disrupt emerging threats and hazards.
4. Manage and reduce systemic risks.
5. Increase understanding of international critical infrastructure interdependencies and anticipate cascading impacts.
6. Influence international policy, standards, and best practices.
7. Assist key partners to address their capability shortfalls.
8. Expand bilateral/multilateral exchanges of expertise, in tandem with increased federal inter- and intra-agency coordination, to improve risk management and incident response capacity.
9. Mature and strengthen CISA's international partnerships, arrangements, and policies.

# 2. OUR GOALS AND OBJECTIVES

## GOAL 1: BOLSTER THE RESILIENCE OF FOREIGN INFRASTRUCTURE ON WHICH THE U.S. DEPENDS

Recognizing that much of U.S. critical infrastructure interconnects and/or is interdependent with foreign assets, systems, or networks, CISA will work closely with domestic and international partners to bolster the security and resilience of the international critical infrastructure on which the U.S. depends. These interconnections and interdependencies span the full range of critical infrastructure sectors: pipelines, telecommunications, and essential supply chains, among others. Malicious cyber actors continue to exploit vulnerabilities across these sectors to target critical infrastructure through ransomware and other cyberattacks. The threat from global terrorism remains a persistent concern and a significant threat to U.S. and international facilities. Thus, it is essential for CISA to work with partners to assess and reduce risk from foreign critical dependencies impacting U.S. critical infrastructure resilience. In doing so, CISA must strengthen exchanges with international partners that promote our priorities abroad as well as influence standards, regulations, and policies to advance homeland and national security objectives. A collaborative approach to understanding interconnected critical infrastructure systems will set conditions for the U.S. and our international partners to proactively develop strategies, policies, and programs that integrate risk reduction efforts and reflect mutual and multi-stakeholder security interests at home and abroad.

### *OBJECTIVES*

**1.1. Identify and prioritize foreign critical infrastructure on which the nation depends and bolster its security and resilience.**
The U.S. depends on foreign-owned systems that support our critical infrastructure sectors such as communications, transportation, information technology, energy, financial services, and critical manufacturing. CISA will work with interagency and international partners to identify and understand which international systems and assets are truly critical to the nation's critical infrastructure and assess how they are vulnerable to create strategies to manage shared risks. CISA will also work with interagency and international partners to promote a shared understanding of global threats to critical infrastructure security and resilience, such as cyberattacks, chemical and improvised explosive devices, threats to supply chain interdependencies, foreign malign investments, and climate change. Managing risk and bolstering resilience will require long-term, strategic collaboration between public and private sectors at home and abroad.

**Enabling Measure:** In coordination with the Department of State and relevant U.S. government partners, we will broaden our understanding of systemic risk by expanding our visibility into infrastructure and supply chain vulnerabilities for priority foreign critical infrastructure upon which the U.S. depends.

**Measure of Effectiveness:**

1. Increase the number of U.S. government activities coordinated by CISA to advance the security and resilience of prioritized foreign critical infrastructure and supply chains.
2. Increase the number of global partner actions taken to address risks to prioritized foreign critical infrastructure.
3. Increase the number of domestic partner actions taken to mitigate potential disruptions of U.S. critical infrastructure operations resulting from dependencies with foreign assets, systems, and supply chains.

### 1.2. Strengthen international partnerships that promote U.S. critical infrastructure priorities and interests abroad.

CISA seeks to expand visibility into internationally shared threats and systemic risks. To improve situational awareness for both CISA and our international stakeholders, we must mature multidirectional communications with external partners, including timely incident reporting and the systematic sharing of threat and vulnerability information. Strengthening includes accelerating the speed, improving the accuracy, and enabling the effectiveness of critical information sharing, while using CISA as a hub for multi-stakeholder initiatives. We will use CISA's cross-functional expertise to foster communication and information sharing with global partners at scale, which will advance the resiliency of our critical infrastructure against shared challenges and preserve our ability to communicate in the event of an emergency. This will create a foundation for advancing international efforts that mature our collective ability to plan for, detect, deter, and disrupt emerging threats and hazards to cyber and physical infrastructure and interoperable emergency communications. Deepening the understanding of shared and systemic risk with our partners will strengthen the protection and resilience of critical infrastructure on which the nation relies.

**Enabling Measure:** We will expand our ability to execute joint operational activities, capacity development efforts, and shared policy frameworks that advance U.S. priorities for defending cyberspace and protecting U.S. critical infrastructure.

**Measure of Effectiveness:**

1. Increase the number of joint operational activities conducted with global partners to build public and private capacity to deter, prevent, protect, and respond to incidents to critical infrastructure.
2. Increase information sharing exchanges with global partners to promote U.S. security and resilience priorities and to enhance CISA's programs, services, and products.

### 1.3. Shape operational and technical global standards, regulations, policies, guidelines, and best practices to advance security.

CISA will work with interagency partners to support standards activities—in coordination with the DHS Science and Technology Directorate—through standard development organizations that can advance U.S. interests. Within CISA's authorities, our aim is to promote and support a wide array of portfolios, including but not limited to cyber and physical critical infrastructure, emerging technology, chemical security, emergency communications, school safety, bombing prevention, and more to ensure that systems, infrastructure, government, business, and the public can withstand and recover from deliberate attacks, accidents, and natural hazards. Where appropriate, we will advance and contribute to the development and adoption of operational and technical international standards and regulations to strengthen cybersecurity, fortify critical infrastructure security and resilience, and improve emergency

communication. CISA holds a shared approach to international standards, regulations, guidelines, and best practices for critical infrastructure security and critical emerging technologies, to include artificial intelligence (AI). This will help accelerate standards that contribute to interoperability and promote U.S. competitiveness and innovation with our partners.

**Enabling Measure:**

1. We will advance open, transparent, and rules-based standards processes to ensure that globally relevant standards meet U.S. national security requirements for critical infrastructure.
2. We will work with partners to counter the influence of adversaries attempting to unduly shape standards in a manner which would represent a threat to national security.

**Measure of Effectiveness:**

1. In coordination with government, industry, and academic partners, increase the development and publication of technical standards for adoption by international standards and policy setting bodies that advance the protection, interoperability, and resilience of U.S. critical infrastructure.

## GOAL 2: STRENGTHEN INTEGRATED CYBER DEFENSE

Cybersecurity threats extend beyond national borders. Strong international cyber defense partnerships set conditions that reduce risk and minimize the impact of attempts to infiltrate, exploit, disrupt, or destroy critical infrastructure systems that support our national critical functions (NCFs). Engaging international partners allows CISA to build trust, illuminate threats, and facilitate the free flow of cybersecurity defense information. We will work with partners, international organizations, and nongovernmental organizations to influence global cybersecurity practices and standards that promulgate cyber safety and security at scale. Bolstering the capabilities of key partners improves our collective cyber defense abroad against state and non-state actors.

### *OBJECTIVES*

**2.1. Enable cyber defense with partners to reduce collective risk.**

International partners contribute essential information to support CISA's cybersecurity mission. A network of trusted partners provides increased visibility into—and ability to mitigate—cybersecurity threats, vulnerabilities, and campaigns. Our aim is to increase and mature our network of trusted partners through our bilateral and multilateral Computer Security Incident Response Team (CSIRT)-CSIRT engagements. Through these engagements, we seek to strengthen CSIRT-CSIRT relationships that enable the exchange of actionable operational information, which includes product sharing, vulnerability alerts, victim notifications, tactics, techniques, and procedures as well as evaluating unique international inputs to reduce risk. This effort will facilitate a collective response and provide a vehicle for partners to share information that builds trust and global cyber situational awareness—especially for those foreign systems, networks, and assets truly vital to the nation's critical infrastructure. We will strive to set an example as the premier CSIRT organization and work with international partners to understand how incidents occur, how to prevent them, and to

provide technical resources that alleviate critical operational gaps. Beyond immediate threat information, these operational partnerships help inform international exercises that will enable us to better understand risks and provide additional ways and means to better manage threats and risk abroad.

**Enabling Measure:** We will increase trust and strengthen operational collaboration through bilateral and multilateral engagements with international partners by expanding participation in CSIRT-CSIRT engagements.

**Measure of Effectiveness:**

1. Increase the number of trusted international CSIRT partners.
2. Increase the percent of bilateral and multilateral CSIRT engagements that reduce combined risk.
3. Increase the number of CSIRT partners that apply recommended risk mitigations prior to exploitation.

### 2.2. Drive standards and security at scale to increase cyber safety.

For decades, the U.S. has worked through international institutions to define and advance responsible state behavior in cyberspace, steering partners toward developing secure technology from inception. As part of the broader national effort, CISA will encourage international partners to define, adopt, and implement global cybersecurity standards, norms, and best practices that promote U.S. cybersecurity interests. The agency will also provide guidance, advice, and expertise to help define and implement safe global standards, norms, and best practices that support U.S. domestic cybersecurity interests. Our aim is to set the bar high for global standards and prioritize them to reflect CISA interests and implement them as a critical element to protect citizens. As some of the most visible examples, CISA's international focus is to encourage the widespread adoption of Secure by Design practices, including adoption of software bills of materials, secure AI systems, open-source security, and coordinated vulnerability disclosures.

**Enabling Measure:** In collaboration with international public and private sector partners, we will advance a global commitment to safe and secure software development and deployment.

**Measure of Effectiveness:**

1. Increase in international standards that recommend frameworks for secure software development at the onset of the software development lifecycle.
2. Increase the number of partner states, international organizations, and industries that adopt and implement the principles of Secure by Design.

### 2.3. Increase cyber and physical resilience capabilities of key partners.

The breadth and depth of the international cybersecurity challenge exceeds the capacity of any one organization. It is paramount that key partners possess the fundamental capabilities to safeguard and defend their connected critical infrastructure that impact our NCFs. Our aim is to establish an environment where our partners can organically detect threats, assess potential impacts, and receive and exchange real-time risk reduction actions that increase collective security and resilience and support the rapid establishment of

consistent, secure, and effective interoperable emergency communications. CISA possesses capabilities that can uniquely contribute to homeland and national security objectives—especially as part of larger U.S. government efforts to improve the cybersecurity capabilities of priority international partners. As the U.S. strengthens relationships with key partners, CISA can provide training, exercises, and information sharing capabilities. These activities can assist international partners in developing and growing organic risk reduction capabilities, while setting supporting priorities for the investment and divestment of limited resources to fill collective capability shortfalls.

**Enabling Measure:** In collaboration with the Department of State, we will advance shared cybersecurity priorities and strengthen international partner capacity to support these priorities through the focused delivery of CISA services that proactively and collaboratively bolster our international cybersecurity and resilience.

**Measure of Effectiveness:**

1. Increase the number of CISA services delivered to international partners that address identified security and resilience gaps.
2. Increase in the percent of program participants equipped with required competencies in cyber or physical security and resilience.
3. Expand the network of foreign train-the-trainer partners capable and approved to provide CISA-based training within their regions.
4. Increase the percent of partners reporting strengthened capabilities to manage their own risk.

## GOAL 3: UNIFY AGENCY COORDINATION OF INTERNATIONAL ACTIVITIES

An effective international plan depends on unity of effort across the agency's divisions and mission enabling offices (offices). Accomplishing unity of effort will require that CISA internally prioritizes, coordinates, deconflicts, and aligns international activities through improved organization and governance, integrated functions, and a well-trained workforce.

### *OBJECTIVES*

**3.1. Strengthen and institutionalize CISA's governance of international activities.**
The CISA Stakeholder Engagement Division (SED) will establish a governance structure to advise on international matters and provide a clear articulation of the agency's international priorities. Taking into account inputs from divisions and offices, these priorities will provide clear guidance that is consistent with CISA's authorities and domestic requirements as well as broader DHS and national security policies.

**Enabling Measure:** We will establish internal agency processes and procedures for governing the agency's international activities using the One CISA approach.

**Measure of Effectiveness:**

1. Increase the number of governance documents and processes that improve standardization

and transparency of agency international activities.

### 3.2. Align and synchronize CISA's international functions, capabilities, and resources.

CISA will support systematic information sharing across the agency through policy coordination and the collection and dissemination of international lessons learned to effectively realize the full range of specialized expertise and capabilities across the agency. SED will coordinate CISA's international communications and activities across CISA to provide the agency with situational awareness of current and projected international activities. This coordination will address gaps and eliminate duplication of effort while ensuring timely execution of operational priorities and alignment of CISA's international activities with this strategic plan and national security priorities.

**Enabling Measure:** We will optimize internal business operations to ensure the coordinated delivery of products and services to international partners that effectively advance cyberspace defense and U.S. critical infrastructure security and resilience.

**Measure of Effectiveness:**

1. Increase the percent of cross-cutting activities coordinated through CISA International Affairs.
2. Increase in internal products and services that improve widespread awareness of key international cybersecurity and critical infrastructure security and resilience issues.

### 3.3. Equip CISA's workforce through training and education to promote CISA's capabilities on the global stage.

With an inherent domestic focus, we recognize that there are skills CISA needs to provide the workforce to influence the international system. CISA will develop and provide training opportunities for employees who will deploy overseas as well as those engaged in deliberate international activities. SED will aim to facilitate DHS and State Department pre-deployment training for Attachés, Liaison Officers, and Technical Advisors deploying overseas, including a CISA familiarization program to ensure a baseline understanding of CISA's organization, role, responsibilities, authorities, and strategic objectives. SED will provide international affairs etiquette guidance to all travelers as part of the travel preparation process. For CISA leadership and travelers conducting potentially sensitive engagements, SED will provide a tailored pre-departure briefing encompassing cultural norms and U.S. foreign policy goals with recommended talking points.

**Enabling Measure:** CISA, through its workforce, is prepared to actively and effectively engage in international efforts to advance cyberspace defense, safe and secure technology development and deployment, and critical infrastructure security and resilience.

**Measure of Effectiveness:**

1. Increase the percent of CISA personnel trained and provided with resources to deliver international services.
2. Increase in the percent of CISA personnel who report that specialized training improved their capability to represent the agency effectively while performing international activities.

# 3. CONCLUSION

Robust and trusted international partnerships serve as a force multiplier across the spectrum of global competition. Successful partnerships require commitment, dedication, and time to build trust. In coordination with DHS and the State Department, CISA will develop, strengthen, and sustain these relationships. This CISA 2025–2026 International Strategic Plan provides a framework to build and maintain an agency posture with international partners to enable the U.S. to compete with and prevail against current and future threats. Importantly, this plan addresses multiple challenges under different conditions and creates the framework to prioritize agency efforts.

These goals position CISA strategically with a posture that reinforces critical partnerships abroad to overcome complex and interconnected challenges. The strategic approach aligns CISA with the broader U.S. government as well as our international partners to enable access, develop capacity, and ensure the flexibility to support national efforts to compete globally against state and non-state actors.

This CISA 2025–2026 International Strategic Plan creates opportunities for shared success and is a process, not simply a publication; therefore, CISA will review progress quarterly. Unpredictability in the international security environment, or obstacles to our progress, may drive us to change course. We will remain agile and shift our focus to ensure we are integrating the right people, processes, technology, and partners at the right time, place, and space for mission success. Just as our threats and adversaries adapt to and shape the cyber and physical security environment, CISA will continue to evolve to fulfill the vision of a secure and resilient infrastructure for the American people—this CISA 2025-2026 International Strategic Plan establishes a proactive path to achieve that vision.

## APPENDIX 1: TERMS OF REFERENCE

**Critical Infrastructure**
Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of those matters, across any federal, state, regional, territorial, or local jurisdiction.

**Dependency**
A directional relationship between two entities (objects, persons, or processes) in which one requires the use of, or inputs from, the other.

**Function**
Service, process, capability, or operation performed by an asset, system, network, or organization.

**Integrated**
The arrangement of unified actions in time, space, and purpose, executed as a whole to address trans-regional, all-domain, and multi-functional challenges to U.S. critical infrastructure.

**Interdependency**
Relationships or connections between entities of different functions, networks, sectors, or services.

**National Critical Function (NCF)**
Functions of government and the private sector that are so vital to the U.S. that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, and national public health or safety, or any combination thereof.

**Resilience**
The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability of systems, infrastructure, government, business, and the general public to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

**Sector**
Collection of assets, systems, networks, entities, or organizations that provide or enable a common function for national security (including national defense and continuity of government), national economic security, national public health or safety, or any combination thereof.

## APPENDIX 2: ALIGNMENT WITH THE CISA STRATEGIC PLAN

| Goal 1: Bolster the Resilience of Foreign Infrastructure on Which the U.S. Depends | CISA Strategic Plan Objective |
|---|---|
| **1.1. Identify and prioritize foreign critical infrastructure on which the nation depends and bolster its security and resilience.** | 1.2. Increase CISA's ability to actively detect cyber threats targeting America's critical infrastructure and critical networks.<br><br>2.1. Expand visibility of risks to infrastructure, systems, and networks. |
| **1.2. Strengthen international partnerships that promote U.S. critical infrastructure priorities and interests abroad.** | 1.4. Advance the cyberspace ecosystem to drive security-by-default.<br><br>2.4. Build greater stakeholder capacity in infrastructure and network security and resilience.<br><br>3.1. Optimize collaborative planning and implementation of stakeholder engagements and partnership activities.<br><br>3.4. Enhance information sharing with CISA's partnership base. |
| **1.3. Shape operational and technical global standards, regulations, policies, guidelines, and best practices to advance security.** | 2.3. Enhance CISA's security and risk mitigation guidance and impact. |

| Goal 2: Strengthen Integrated Cyber Defense | CISA Strategic Plan Objective |
|---|---|
| **2.1. Enable cyber defense with partners to reduce collective risk.** | 1.3. Drive the disclosure and mitigation of critical cyber vulnerabilities.<br>2.5. Increase CISA's ability to respond to threats and incidents.<br>3.4. Enhance information sharing with CISA's partnership base. |
| **2.2. Drive standards and security at scale to increase cyber safety.** | 1.4. Advance the cyberspace ecosystem to drive security-by-default. |
| **2.3. Increase cyber and physical resilience capabilities of key partners.** | 2.4. Build greater stakeholder capacity in infrastructure and network security and resilience.<br>3.5. Increase integration of stakeholder insights to inform CISA product development and mission delivery. |

| Goal 3: Unify Agency Coordination of International Activities | CISA Strategic Plan Objective |
|---|---|
| **3.1. Strengthen and institutionalize CISA's governance of international activities.** | 4.1. Strengthen and integrate CISA governance, management, and prioritization. |
| **3.2. Align and synchronize CISA's international functions, capabilities, and resources.** | 2.1. Expand visibility of risks to infrastructure, systems, and networks.<br><br>3.3. Streamline stakeholder access to and use of appropriate CISA programs, products, and services.<br><br>4.2. Optimize CISA business operations to be mutually supportive across all divisions. |
| **3.3. Equip CISA's workforce through training and education to promote CISA's capabilities on the global stage.** | 4.3. Cultivate and grow CISA's high-performing workforce. |