United States of America

Last Updated: December 2021

CYBERSECURITY POLICY

Strategy Documents

Memorandum on Space Policy Directive 7

The White House

- Establishes implementation actions and guidance for U.S. space-based positioning, navigation and timing (PNT) programs and activities for national and homeland security, civil, commercial and scientific purposes;
- The SPD-7 supersedes the 2004 National Security Presidential Directive-39, "United States Space-Based Positioning, Navigation, and Timing Policy";
- Mentions cyber in context of navigation warfare (NAVWAR); focus on importance of improving the cybersecurity of GPS.

Source Source 2

15 January 2021

Department of Defense Outside the Continental United States (OCONUS) Cloud Strategy

Office of the DoD Chief Information Officer

- The Strategy establishes the vision and goals for enabling a dominant all-domain advantage through cloud innovation at the tactical edge.
- It identifies areas that require modernisation to realise the potential of cloud computing in the direct support of warfighter, specifically:
  - security
  - redundancy
  - reliability
  - availabity

Source

April 2021

Executive Order on Improving the Nation's Cybersecurity

The White House

- President Biden released the Executive Order on Improving the Nations Cybersecurity in May 2021;
- The executive order followed a series of high-profile information security attacks and ransomware incidents targeting the public and private sector.
- The EO charges multiple agencies; including NIST; with enhancing cybersecurity through a variety of initiatives related to the security and integrity of the software supply chain.

Source

12 May 2021

National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems

the White House

- The memorandum directs the Department of Homeland Security (DHS) to work with the Department of Commerce (DOC) in developing cybersecurity performance goals that will drive adoption of effective practices and controls. NIST will play a role in that collaboration.

Source

28 July 2021

Cybersecurity Principles for Space Systems (Space Policy Directive-5)

Cybersecurity and Infrastructure Security Agency (CISA)

SPD-5 establishes the following key cybersecurity principles of space systems:

- Space systems and their supporting infrastructure including software, should be developed and operated using risk-based, cybersecurity-informed engineering;
- Space systems operators should develop or integrate cybersecurity plans for space systems that include capabilities to ensure operators or

automated control center systems can retain or recover positive control of space vehicles, and verify the integrity, confidentiality, and availability of critical functions and the missions, services, and data they provide;
- Space system cybersecurity requirements and regulations should leverage widely-adopted best practices and norms of behavior;
- Space system owners and operators should collaborate to promote the development of best practices and mitigations to the extent permitted by law and regulation; and,
- Space systems security requirements should be designed to be effective while allowing space operators to manage appropriate risk tolerances and minimize undue burden to civil, commercial, and other non-government space system operators.

Source

September 2020

National Strategy to Secure 5G of the United States of America
The White House

This National Strategy to Secure 5G will fulfill the goals of the National Cyber Strategy with four lines of effort: (1) facilitating the rollout of 5G domestically; (2) assessing the cybersecurity risks to and identifying core security principles of 5G capabilities and infrastructure; (3) addressing risks to United States economic and national security during development and deployment of 5G infrastructure worldwide; and (4) promoting responsible global development and deployment of secure and reliable 5G infrastructure.

Source Source 2

March 2020

Federal Cybersecurity Research and Development Strategic Plan
Office of Science and Technology Policy; Subcommittee on Networking & Information Technology Research & Development; Cyber Security and Information Assurance Interagency Working Group of the National Science and Technology Council (NSTC)

The Plan identifies four interrelated defensive capabilities (deter, protect, detect, and respond) and six priority areas for cybersecurity R&D (artificial intelligence, quantum information science, trustworthy distributed digital infrastructure, privacy, secure hardware and software, and education and workforce development).

The 2019 Federal Cybersecurity Research and Development Strategic Plan supersedes Federal Cybersecurity Research and Development Strategic Plan from 2016.

Source Source 2

December 2019

Cloud Strategy
Department of Defense

- Recognizes the cloud as a fundamental component of the global infrastructure that will empower the warfighter with data and is critical to maintaining the military's technological advantage;
- Focuses implementation activities on two fundamental types of work: (1) the stand up of cloud platforms ready to receive data and applications, and (2) the ongoing work to migrate existing applications and to develop new applications in the cloud;
- Identifies seven strategic objectives:

1. Enable exponential growth;
2. Scale for the episodic nature of the DoD mission (Elasticity):
3. Proactively address cyber challenges;
4. Enable data and AI transparency;
5. Extend tactical support for the warfighter at the edge;
6. Take advantage of resiliency in the cloud; and
7. Drive IT reform at DoD.

Source

December 2018

National Cyber Strategy of the United States of America
The White House

Structured around four pillars of the National Security Strategy:

• Protect the American people, homeland, and the American way of life;
• Promote American prosperity;
• Preserve peace through strength;
• Advance American influence.

Source Source 2

20 September 2018

Cybersecurity Strategy
Department of Homeland Security

Five pillars:

- Risk identification;
- Vulnerability reduction;
- Threat reduction;
- Consequence mitigation;
- Enable cybersecurity outcomes.

The department plans to review and update the strategy in 2023.

Source

15 May 2018

The DOD Cyber Strategy 2018
Department of Defense (DOD)

The Department’s cyberspace objectives are:

1. Ensuring the Joint Force can achieve its missions in a contested cyberspace environment;

2. Strengthening the Joint Force by conducting cyberspace operations that enhance U.S. military advantages;

3. Defending U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident;

4. Securing DoD information and systems against malicious cyber activity, including DoD information on non-DoD-owned networks; and

5. Expanding DoD cyber cooperation with interagency, industry, and international partners.

Source

2018

National Defense Strategy (NDS) 2018
Department of Defense (DOD)

Defense objectives include:

- Defending the homeland from attack;
- Sustaining Joint Force military advantages, both globally and in key regions;
- Deterring adversaries from aggression against our vital interests;
- Enabling U.S. interagency counterparts to advance U.S. influence and interests;
- Maintaining favorable regional balances of power in the Indo-Pacific, Europe, the Middle East, and the Western Hemisphere;
- Defending allies from military aggression and bolstering partners against coercion, and fairly sharing responsibilities for common defense;
- Dissuading, preventing, or deterring state adversaries and non-state actors from acquiring, proliferating, or using weapons of mass destruction;
- Preventing terrorists from directing or supporting external operations against the United States homeland and our citizens, allies, and partners overseas;
- Ensuring common domains remain open and free;
- Continuously delivering performance with affordability and speed as we change Departmental mindset, culture, and management systems; and

- Establishing an unmatched twenty-first century National Security Innovation Base that effectively supports Department operations and sustains security and solvency.

Source Source 2

2018

National Security Strategy of the United States of America (NSS)

The White House and Cabinet

• Identifies need to protect critical infrastructure and go after malicious cyber actors.
• Strengthen capabilities—including in space and cyberspace—and revitalize others that have been neglected
• Deploy layered defenses, improve information sharing and sensing, build defensible government networks
• Notes response to the challenges and opportunities of the cyber era will determine future prosperiy and security
• Improve attribution, accountability, and response
• Enhance cyber tools and expertise
• Improve integration and agility (between government bodies)

Source Source 2

December 2017

Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government

Office of Management and Budget

Five objectives of CSIP are:

1. Prioritized Identification and Protection of high value information and assets;
2. Timely Detection of and Rapid Response to cyber incidents;
3. Rapid Recovery from incidents when they occur and Accelerated Adoption of lessons learned from the [Cybersecurity] Sprint assessment;
4. Recruitment and Retention of the most highly-qualified Cybersecurity Workforce talent the Federal Government can bring to bear; and
5. Efficient and Effective Acquisition and Deployment of Existing and Emerging Technology.

Source

30 October 2015

Presidential Policy Directive 41 (PPD-41) – United States Cyber Incident Coordination

The White House

Outlines unity of effort within the Federal Government and close coordination between the public and private sectors to cyber incidents.

Source

July 2016

Executive Order 13984 – Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities

The White House

- Amends and expands Executive Order 13694 of April 1, 2015, to detect and deter the use of US infrastructure as a service (“IaaS”) products by foreign malicious cyber actors;
- Directs the US Department of Commerce (“Commerce”) to (i) issue regulations to detect and deter the use of US IaaS products in malicious cyber-enabled activities primarily via identity verification requirements and to (ii) coordinate with other US government agencies to impose “special measures” against certain foreign persons and/or foreign jurisdictions.

Source Source 2

19 January 2021

Executive Order 13870 – on America's Cybersecurity Workforce (EO 13870)

The White House

The EO on America's Cybersecurity Workforce supports building and sustaining a strong Federal cybersecurity workforce.

Source Source 2

2 May 2019

Executive Order 13800 – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (EO 13800)

The White House

Consists of:

- Improving the security of federal government computer networks;
- Leveraging government resources to better secure critical infrastructure;
- Establishing norms of good behavior in cyberspace and punishing bad behavior.

Source Source 2

11 May 2017

Executive Order 13636 – Improving Critical Infrastructure Cybersecurity (EO 13636)

The White House

Consists of increasing the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities.

Source

12 February 2013

Implementation Frameworks

FY2021 Federal Cybersecurity R&D Strategic Plan Implementation Roadmap

Executive Office of the President of the United States

Source

14 August 2020

National Strategy to Secure 5G Implementation Plan

National Telecommunications and Information Administration, Department of Commerce

In accordance with the Secure 5G and Beyond Act of 2020, the Executive Branch has developed a comprehensive implementation plan associated with the National Strategy to Secure 5G.

Source Source 2

6 January 2021

National Maritime Cybersecurity Plan to the National Strategy for Maritime Security

The White House

Document outlines the National Maritime Cybersecurity Plan as an addendum to the National Strategy for Maritime Security.

Source Source 2

December 2020

Automated Indicator Sharing (AIS)

Department of Homeland Security (DHS)

The AIS enables the real-time exchange of machine-readable cyber threat indicators and defensive measures to help protect participants of the AIS community and ultimately reduce the prevalence of cyberattacks.

Source

1 March 2016

Framework for Improving Critical Infrastructure Cybersecurity

National Institute of Standards and Technology

Focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization’s risk management processes

Source

12 February 2014

The Comprehensive National Cybersecurity Initiative (CNCI)

The White House

Comprises 12 Initiatives with three main goals:

- To establish a front line of defense
- To defend against the full spectrum of threats
- To strengthen the future cybersecurity environment

Source

January 2008

STRUCTURE

National Centre or Responsible Agency

Cybersecurity and Infrastructure Security Agency (CISA)

Department of Homeland Security

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation’s risk advisor, working with partners to defend against today’s threats and collaborating to build more secure and resilient infrastructure for the future. CISA builds the national capacity to defend against cyber attacks and works with the federal government to provide cybersecurity tools, incident response services and assessment capabilities to safeguard the ‘.gov’ networks that support the essential operations of partner departments and agencies.

Source Source 2

Key Positions

Director

Cybersecurity and Infrastructure Security Agency (CISA)

Source Source 2

Dedicated Agencies and Departments

Office of Cyber and Infrastructure Analysis (OCIA)

Department of Homeland Security

Responsible for supporting efforts to protect the Nation's critical infrastructure through an integrated analytical approach evaluating the potential consequences of distruption from physical or cyber threats and incidents.

Source

Cyber Threat Intelligence Integration Center (CTIIC)

Office of the Director of National Intelligence

Build understanding of foreign cyber threats to US national interests to inform decision-making by federal cyber centers, departments and agencies, and policy makers.

Source Source 2

February 2015

Cybersecurity Unit

Computer Crime and Intellectual Property Section, Department of Justice

Central hub for expert advice and legal guidance regarding how the criminal electronic surveillance and computer fraud and abuse statutes impact cybersecurity

Source Source 2

December 2014

Cyber Security Division

Cybersecurity & Infrastructure Security Agency (CISA)

Leads efforts to protect the federal ".gov" domain of civilian government networks and to collaborate with the private sector - the ".com" domain - to increase the security of critical networks. This occurs through the following functions:

- Capability Delivery
- Threat Hunting
- Operational Collaboration
- Vulnerability Management
- Capacity Building
- Strategy, Resources & Performance
- Cyber Defense Education & Training

Source Source 2

National Cybersecurity and Communications Integration Center (NCCIC)

Office of Cybersecurity and Communications

Composed of NCCIC Operations & Integration, US-CERT, Industrial Control Systems Cyber Emergency Response Team, and National Coordinating Center for Communications

Source Source 2

October 2009

United States Cyber Command (Cybercom)

National Security Agency

Centralizes command of cyberspace operations, strengthens DoD cyberspace capabilities, and integrates and bolsters DoD's cyber expertise.

Source Source 2

2009

National Cyber Investigative Joint Task Force (NCIJTF)
Federal Bureau of Investigation

Coordinate, integrate, and share information to support cyber threat investigations, supply and support intelligence analysis, and provide value to other ongoing efforts.

Source Source 2

2008

National CERT or CSIRT

United States Computer Emergency Readiness Team (US-CERT)
National Cybersecurity and Communications Integration Center

- Responds to major incidents, analyzes threats, and exchanges critical cybersecurity information with trusted partners around the world;
- Governmental CERT.

Source Source 2

2000 (as FedCIRC)

LEGAL FRAMEWORK

Legislation

Secure 5G and Beyond Act of 2020

Source Source 2

23 March 2020

Cybersecurity and Infrastructure Security Agency Act of 2018

Source Source 2

16 November 2018

National Institute of Standards and Technology (NIST) Small Business Cybersecurity Act

Directs the NIST Director to disseminate clear and concise resources, defined as guidelines, tools, best practices, standards, methodologies, and other ways of providing information
Source

13 August 2018

Cybersecurity Act of 2015

Authorizations for preventing, detecting, analyzing, and mitigating cybersecurity threats
Source

18 December 2015 (became Public Law No: 114-113)

Cybersecurity Information Sharing Act (CISA) of 2015

Requires the Director of National Intelligence and DHS, Defense, and Justice to develop procedures to share cybersecurity threat information with private entities, nonfederal government agencies, state, tribal, and local governments, the public, and entities under threat

Source Source 2

18 December 2015

National Cybersecurity Protection Act of 2014

The National Cybersecurity Protection Act of 2014 allows the Department of Homeland Security (DHS) to share information with the private sector, respond to cyber incidents, assist private companies and federal agencies alike, and recommend cyber security measures.

Source Source 2

December 2014

Cybersecurity Enhancement Act of 2014

Aims to provide for an ongoing, voluntary public-private partnership to improve cybersecurity, and to strengthen cybersecurity research and development, workforce development and education, and public awareness and preparedness, and for other purposes.

Source Source 2

18 December 2014 (became Public Law No 113-274)

Electronic Communications Privacy Act (18 USC 2510-22)

Implement and extend government restrictions regarding the use of wire taps on telephone calls and transmissions of electronic data by way of computer

Source

1986; 10 July 2008 (amended)

Computer Fraud and Abuse Act (18 USC 1030)

Prohibits accessing a computer without authorization, or in excess of authorization

Source Source 2

1986

Views on International Law

Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266

The Group of Governmental Experts established pursuant to the he General Assembly resolution 73/266, adopted its report by consensus on 28 May 2021. In paragraph 73 of the Group’s report (A/76/135), it is stated that, in accordance with the Group’s mandate, an official compendium of voluntary national contributions of participating governmental experts on the subject of how international law applies to the use of ICTs by States will be made available on the website of the Office for Disarmament Affairs.

Source

May 2021

COOPERATION

Multilateral Agreements

Budapest Convention

PARTY

Source Source 2

1 January 2007 (entry into force)

UN Processes

Represented at the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

Source

2004, 2009, 2012/2013, 2014/2015, 2016/2017, 2019/2021

Expressed views to the Annual Report of the UN Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security

Source

2011

Expressed Views at the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security

Source Source 2

2019/2020

Bilateral and Multilateral Cooperation

United States – Georgia Memorandum of Understanding on 5G Security

Source Source 2

14 January 2021

Memorandum of Understanding (MoU), US – Singapore

David Koh, Chief Executive of the Cyber Security Agency of Singapore (CSA) and Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency (CISA)

The MoU will focus on:

- Strengthening information sharing;
- Fostering cybersecurity exchanges between Singapore and the U.S.; and
- Cooperation through joint exercises;
- It will also expand into new areas of cooperation such as critical technologies, and research and development.

Source Source 2

August 2021

U.S. – Ukraine Third Cyber Dialogue

The Department of State

- The Third Cyber Dialogue reaffirms our shared commitment to ensure an open, interoperable, reliable, and secure cyberspace in which all states behave responsibly.

Source

3 March 2020

United States of America

Last Updated: December 2021

ASEAN – U.S. Cyber Policy Dialogue

- The Dialogue was co-chaired by the United States and Indonesia.
- The Dialogue demonstrated strong partnership and a shared vision of an open, peaceful, interoperable, reliable, and secure cyberspace that supports international trade and commerce, strengthens international security, and fosters economic prosperity, free expression, and innovation.

Source

8 October 2021

Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting

The White House

Source

13-14 October 2021

U.S.-U.K. Cooperation

President Joe Biden and Prime Minister Boris Johnson

- The two nations will work together to further strengthen and modernise NATO, and increase its common funding, so the Alliance can harness the full range of military and non-military capabilities to tackle existing and emerging threats, including malicious cyber activity and attacks.

Source

10 June 2021

Joint Statement on Japan-U.S.-Brazil Trilateral Exchange

- Aims to bolster existing cooperation to strengthen business environments, expand foreign investments, promote regional connectivity, support sustainable development and economic growth, and enhance cybersecurity to promote vibrant digital economies based on an open, interoperable, reliable, and secure internet.

Source

10 November 2020

U.S.-Chile Cyber Threats Cooperation Agreement

Defense Secretary

Enhance defense and cooperation, specifically on cyber operations and protection of Chile's cyber domain

Source Source 2

16 August 2018

Discussions, Armenia-U.S.

Principal Deputy Assistant Secretary, Bureau of Economic and Business Affairs

Potential cooperation in supporting the Armenian Government on cyber-security and digitization issues.

Source

6 March 2018

Meeting, Croatia-U.S.

FBI

Underlined, inter alia, the need to develop national capacity and international cooperation in cyber security.

Source

18 January 2018

Hemispheric Forum on International Cooperation Against Cybercrime (organizer)

Department of Justice, Department of Homeland Security

Aimed at permitting participating countries to make better use of capacity building programmes of international organizations, to enhance cooperation and synergies between international organizations and initiatives, and to share experience on the strengthening of capacity building for criminal justice authorities

Source

5-7 December 2017

Meeting, Sudan-U.S.

Department of State

Agreement during the meeting on the importance of considering reaching settlement and legalization of the status of US software in Sudan, coordination of efforts concerning information security and prevention of electronic crime.

Source

12 October 2017

U.S.-China Law Enforcement and Cybersecurity Dialogue (First)

Department of Justice, Department of Homeland Security

Continue implementation on U.S.-China cybersecurity cooperation (reached by Heads of States in 2015)

Source

4 October 2017

U.S.-Ukraine Cybersecurity Dialogue (First)

Department of State

Support the development of a framework of responsible state behavior

Source

29 September 2017

Nordic-Baltic Eight (NB8)-US Roundtable on Cyber Security

Source Source 2

27 September 2017

Joint Cyber Security and Software Engineering Research Site, Finland-U.S.

Source

September 2017

Sweden-U.S. Bilateral Meeting

Department for Homeland Security

Yearly bilateral meeting, including workshops focusing on Cyber Security.

Source

28-29 June 2017

Japan-U.S. Cyber Dialogue (Fifth)

Department of State

Focusing on: (1) information sharing and (2) enhancing national efforts

Source

20-21 July 2017

U.S.-Kenya Cyber and Digital Economy Dialogue

Department of State

Meeting focused on the future of the digital economy and protecting the opportunities it presents by combatting cybercrime and promoting cybersecurit

Source

27 June 2017

Memorandum of Understanding, Italy-U.S.

Secret Service

Sets up an international task force to combat cyber crime.

Source

29 June 2009

Cooperation, U.S.-Nigeria

Ambassador to Nigeria

- Cooperation in combatting cybercrime and financial fraud;
- 2nd Annual Conference on Combatting Financial Fraud, Cybercrime, and Cross-Border Crimes.

Source

23 May 2017

US-Argentina Cyber Policy Working Group (inaugural meeting)

Department of State

Meeting focused on key cybersecurity initiatives including implementing national cyber policy frameworks, protecting networks, developing a cyber workforce, and managing cyber incidents

Source

23 May 2017

U.S.-Netherlands Bilateral Call for Proposals in Cyber Security

Cyber Security Division, Science and Technology Directorate, Department of Homeland Security

U.S.-Netherlands bilateral call to provide funding for collaborative cybersecurity research projects conducted by joint US-Dutch teams.

Source

18 May 2017

Cooperation, Belarus-U.S.

Chargé d'affaires

Intensification of cooperation in cybersecurity and copyright protection.

Source

7 February 2017

Memorandum of Understanding, India-U.S.

Department of Homeland Security

Promote closer co-operation and the exchange of information, between CERTs

Source

11 January 2017; 19 July 2011 (previous)

U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues (Third)

Department of Justice, Department of Homeland Security

- Review the timeliness and quality of responses to requests for information and assistance with respect to cybercrime or other malicious cyber activities
- Enhance pragmatic bilateral cooperation with regard to cybercrime, network protection and other related issues

Source

7 December 2016

Republic of Korea-United States Cyber Policy Consultation (Fifth)

Deputy Assistant Secretary of State for Cyber and International Communications and Information Policy Robert Strayer (head of the US delegation), officials from the Department of State, the Department of Commerce, the Department of Defense, and the Federal Bureau of Investigation

- The two countries assessed the cyber security environment; shared international trends in cyber policy and related information; and discussed ways to increase cyber cooperation between the two countries, prospects for discussions on international regulations on cyberspace, and confidence-building measures (CBM) and capacity building.

Source

21 June 2018

Sixth E.U.-U.S. Cyber Dialogue

Government of the United States of America

- The US nd the EU reaffirmed their commitment to a global, open, stable and secure cyberspace where the rule of law is fully respected, where the same rights that individuals have offline are also protected online, and where the security, economic growth, prosperity, and integrity of free and democratic societies is promoted and preserved.

Source

21 June 2019

45th Portugal-US Standing Bilateral Commission (SBC)

- Committed to strong Transatlantic ties and shared values which contribute to mutual prosperity and security;
- The discussion underscored cooperation and an exchange of views on bilateral and international priorities, such as recovery from the COVID-19 pandemic, cyber security, trade, climate and energy, Indo-Pacific, China, Africa, Latin America, as well as NATO, security, and defense matters.
- The SBC noted the importance of digital transition for economic recovery; it underscored the need to fortify cybersecurity, secure 5G networks, and ensure safe, secure, and trusted cross-border data flows with appropriate privacy protections, including by using only trusted providers in our telecommunications networks.

Source

28 July 2021

Australia-U.S. Cyber Security Dialogue (First)

Head of State

Engage senior representatives from both countries’ business, academic and government sectors to discuss common cyber threats, promote cyber security innovation and shape new business opportunities

Source

22 September 2016

U.S.-France Cyber Bilateral Meeting (First)

Department of State

- Increased collaboration on strategic and operational objectives
- Discussions on countering use of the Internet for terrorist and criminal purposes

Source

8-9 September 2016

Memorandum of Understanding, U.K.-U.S.

Secretary of Defense

Joint research into offensive and defensive cyber

Source

September 2016

Framework for the U.S.-India Cyber Relationship

Department of State

Provides shared principles and main areas of cooperation

Source

30 August 2016

Memorandum of Understanding, Singapore-U.S.

Cooperation through regular CERT-CERT information exchanges and sharing of best practices, coordination in cyber incident response and sharing of best practices on Critical Information Infrastructure protection, cybersecurity trends and practices

Source

July 2016

Joint Statement of Intent, Republic of Korea-United States

Science and Technology Directorate, Department of Homeland Security

Agreement "to explore areas of mutual value and benefit, which may lead to joint activities aimed at enhancing operational readiness to support cybersecurity, and resilience,

Source

2 May 2016

Joint Statement on U.S.-Germany Cyber Bilateral Meeting (Fourth)

Department of State

Strategic objectives include affirming common approaches to promoting international cyber security, multistakeholder Internet governance, Internet freedom and the promotion of human rights online; partnering with the private sector to protect critical infrastructure; and pursuing cyber capacity building efforts in third countries

Source

22-23 March 2016

Workshop, Mozambique-U.S.

Department of Justice; Department of State

- Co-organization of a cybersecurity and cybercrime workshop for Lusophone Africa.

Source

22-24 September 2015

U.S.-China Cyber Agreement

The White House

Agree to cooperate with requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory

Source

September 2015

Cybersecurity and Cybercrime Workshop for ECOWAS

Ambassador to the Democratic Republic of Congo

- Partnership between the Governments of the US and DRC
- Address broad issues of cybercrime and cybersecurity while focusing on issues of specific interest to the Central African region such as combating cybercrime; mobile phone security; Internet freedom, access, and affordability; and the development of national computer emergency readiness teams, or CERTs.

Source

24-26 August 2015

Meeting, Peru-U.S.

Southern Command

2nd bilateral meeting in cyberdefense and cybersecurity.

Source

20-22 January 2015

Global Forum on Cyber Expertise (GFCE), Member

A global platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building.

Source Source 2

2015 (member since)

Global Forum on Cyber Expertise, Member

A global platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building

Source

2015 (established)

U.S.-Estonia Cyber Partnership Statement

Department of State

Three elements to partnership:

1. Cooperation in cyber security and cyber defence
2. Bilateral collaboration in law enforcement, academic exchanges, etc.
3. Coordination on capacity building with third parties

Source

3 December 2013

Cybersecurity Action Plan Between Public Safety Canada and the Department of Homeland Security (U.S.)

Department of Homeland Security

Three goals:

1. Enhanced cyber incident management collaboration
2. Engagement and information sharing with private sector
3. Continued cooperation on public awareness

Source Source 2

26 October 2012

Select Activities

National Cyber Security Awareness Month (NCSAM)

Department of Homeland Security (DHS) and the National Cyber Security Alliance (NCSA)

Engage and educate public and private sector partners through events and initiatives.

Source

Since October 2004 (17th year)

30-Day Cybersecurity Sprint

Federal Chief Information Officer

30-day review of the Federal Government’s cybersecurity policies, procedures, and practices

Source

June 2015

Membership

Group of Seven (G7)

International Telecommunications Union (ITU)

North Atlantic Treaty Organization (NATO)

Organization for Security and Co-operation in Europe (OSCE)

Organization of American States (OAS)

United Nations (UN)