United States Government Accountability Office

Report to Congressional Addressees

January 2024

CYBER DIPLOMACY

State's Efforts Aim to Support U.S. Interests and Elevate Priorities

GAO-24-105563

GAO Highlights

Highlights of GAO-24-105563, a report to congressional addressees

Why GAO Did This Study

The U.S. and its allies face intensifying foreign cyber threats as international trade, communication, and critical infrastructure grow more dependent on digital technology. State and non-state actors are using cyberspace increasingly as a platform for irresponsible behavior to undermine democracies. The Department of State leads U.S. government international efforts to advance U.S. interests in cyberspace. In April 2022 State stood up CDP with a mission to address national security challenges, economic opportunities, and implications to U.S. values associated with cyberspace, digital technologies, and digital policy.

The James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 includes a provision for GAO to review U.S. diplomatic efforts to advance interests in cyberspace and other related matters. This report examines, among other things, (1) activities State is undertaking to advance U.S. interests regarding cyberspace, including the use of international agreements and fora, and (2) the extent to which organizational changes have helped position or presented challenges for State to achieve its cyber diplomacy goals.

To identify State's activities, GAO analyzed program documents and discussed implementation of strategic objectives with officials from State. To examine State's organizational changes, GAO analyzed documentation of State's reform plans and implementation, and evaluated the extent to which State addressed selected practices identified by GAO as important to reform.

View GAO-24-105563. For more information, contact Latesha Love-Grayer at (202) 512-4409 or lovegrayerl@gao.gov.

January 2024

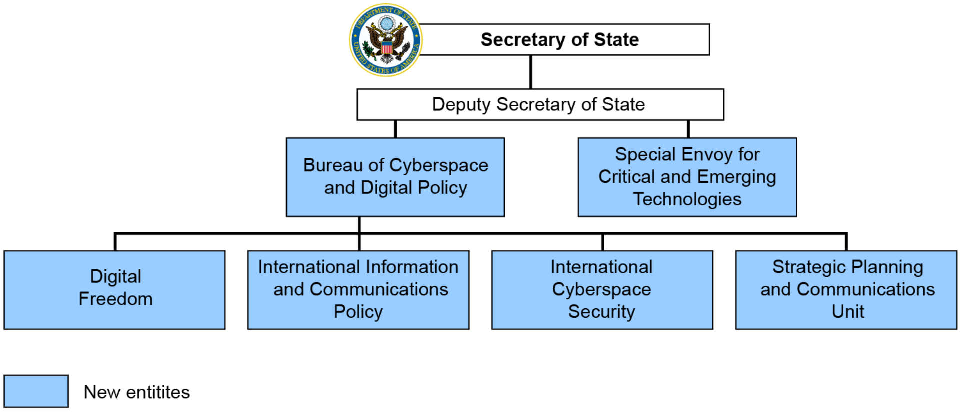
CYBER DIPLOMACY

State's Efforts Aim to Support U.S. Interests and Elevate Priorities

What GAO Found

The Department of State (State) conducts a range of diplomatic and foreign assistance activities intended to support objectives identified in the 2023 National Cybersecurity Strategy. Specifically, State engages in multilateral fora and agreements that aim to strengthen norms of responsible state behaviors, deter unacceptable state behaviors, and advance cyber policies. For example, State worked with the United Nations Group of Governmental Experts and Open-Ended Working Group to develop a framework on behavior in cyberspace, including a set of peacetime norms and confidence building measures. According to State officials, establishing cyber norms, including enforcing consequences for rule-breakers, raises the cost of bad behavior in cyberspace and deters wrongdoing. State also engages in bilateral activities to promote U.S. aligned cyber norms and policies, such as working with Denmark to advance the Copenhagen Pledge on Tech for Democracy. This pledge intends to counter authoritarian repression of free speech online and advance digital freedom globally. In addition, State provides foreign assistance, such as training and technical assistance, to strengthen partner capacity all over the world.

New Entities State Created to Elevate Cyber Priorities


Secretary of State
Deputy Secretary of State
Bureau of Cyberspace and Digital Policy
Special Envoy for Critical and Emerging Technologies
Digital Freedom
International Information and Communications Policy
International Cyberspace Security
Strategic Planning and Communications Unit
New entitites

Source: GAO based on Department of State documentation (data); Department of State (seal). | GAO-24-105563

State established the Bureau of Cyberspace and Digital Policy (CDP) in April 2022 to elevate cyber priorities and is taking steps to address some of the challenges the new bureau faces as it works to promote U.S. cyber interests. State consolidated its efforts and leadership of cyberspace-related activities into CDP—a single unit led by an Ambassador-at-Large. Previously, several entities within State shared responsibility for cyber diplomacy. GAO found that this change has helped to better position State to achieve its cyber diplomacy goals. For example, CDP's ambassador level leadership has enabled engagement with higher levels of foreign government officials and raised the U.S. profile on cyber globally. GAO also found that State addressed relevant leading reform practices when forming the Bureau. For example, State has an implementation team dedicated to addressing capacity staffing, resources, and change management. CDP still faces challenges as it pursues cyber goals under the reformed structure, such as needing to clarify roles between the bureau and its partners. However, CDP officials identified steps that they are taking to address them.

United States Government Accountability Office

Contents

Tables

Figures

Abbreviations

CDP	Bureau of Cyberspace and Digital Policy
DCCP	Digital Connectivity and Cybersecurity Partnership
DRL	Bureau of Democracy, Human Rights, and Labor
FOC	Freedom Online Coalition
GGE	Group of Governmental Experts
GLEN	U.S. Transnational and High-Tech Crime Global Law Enforcement Network
INL	Bureau of International Narcotics and Law Enforcement Affairs
ITU	International Telecommunication Union
OAS	Organization of American States
OEWG	Open Ended Working Group
S/TECH	Office of the Special Envoy for Critical and Emerging Technology
TTC	Trade and Technology Council
UN	United Nations

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

January 11, 2024

Congressional Addressees

The U.S. and its allies face intensifying foreign cyber threats underscored by the war in Ukraine, competition with China, and conflicts with Russia, as international trade, communication, and critical infrastructure grow increasingly dependent on digital technology. State and non-state actors are increasingly using cyberspace as a platform for irresponsible behavior from which to target critical infrastructure and our citizens, undermine democracies and international institutions and organizations, and undercut fair competition in our global economy by stealing ideas when they cannot create them. Russia's aggressive cyberattacks on civilian infrastructure and disinformation campaigns conducted during the war in Ukraine illustrate the risk. At the same time, the global arena presents positive opportunities for the U.S. to instill its key values into the digital ecosystem, including the belief in the potential of digital technologies to promote connectivity, democracy, peace, the rule of law, sustainable development, and the enjoyment of human rights and fundamental freedoms.

The Department of State (State) leads U.S. government international efforts to advance U.S. interests in cyberspace. In October 2021, Secretary of State Blinken remarked that on cyberspace and emerging technologies, the United States has a major stake in shaping the digital cyber revolution and in making sure that it serves our people, protects our interests, boosts our competitiveness, and upholds our values. State's cyber diplomacy strategic objectives include building coalitions, strengthening capacity, and reinforcing norms. To help achieve those objectives, State stood up a new Bureau of Cyberspace and Digital Policy (CDP) in April 2022.

The James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 included a provision for us to review U.S. diplomatic efforts to advance its interests in cyberspace and other related matters.[1] We also received a separate request to review these topics. This report examines: 1) activities State is undertaking to implement its strategy for cyber diplomacy, including the use of, international agreements and fora, and what has been reported about their impact, and 2) the extent to which

[1] Pub. L. No. 117-263, § 9504, 136 Stat. 3903 (Dec. 23, 2022).

organizational changes have helped position or presented challenges for State to achieve its cyber diplomacy goals.

To identify activities State is undertaking to advance U.S. interests regarding cyberspace, we focused on ongoing and recently concluded activities from 2020 through 2023. We analyzed program documents and discussed strategic objectives and their implementation with officials from State and relevant agencies, including the United States Agency for International Development (USAID), Department of Defense (DOD), and Department of Homeland Security (DHS). We reviewed results of selected programs and spoke with State officials to determine what has been reported about their impact.

To examine the extent to which organizational changes helped position or presented challenges for State to achieve its cyber diplomacy goals, we analyzed the establishment of CDP by examining documentation of State's rationale, implementation, plans, and organizational changes. We evaluated the organizational changes by assessing the extent to which State addressed selected government reform practices, outlined in prior GAO work.[2] We also identified key examples of the benefits that State has gained from the formation of the new consolidated bureau and its high-level leadership. For more details on our scope and methodology, see appendix I.

We conducted this performance audit from November 2021 to January 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Description of Cyber Diplomacy

The term "cyber diplomacy" encompasses a wide range of U.S. interests in cyberspace. According to State officials and nongovernmental organization (NGO) representatives, no official definition of cyber diplomacy exists. In this report, we consider "cyber diplomacy" to be efforts that support U.S. interests in cyberspace internationally, led by the

[2] GAO, *Government Reorganization: Key Questions to Assess Agency Reform Efforts*, GAO-18-427 (Washington, D.C.: June 13, 2018).

Department of State. These efforts involve providing U.S. foreign assistance to partner nations and engaging in multilateral and bilateral interactions, including activities aimed at combatting cybercrime, establishing norms of responsible behavior in cyberspace, and developing technical standards. CDP plays a lead role at State in conducting cyber diplomacy through leadership, management, or support of a range of cyber diplomacy activities. State officials told us the department's view of cyber diplomacy includes advancing a positive vision for an interoperable and reliable global internet through diplomatic efforts. Such efforts work to reduce the risk of conflict for the U.S. and its partners, and to achieve security and stability in cyberspace.

Prior GAO Work on Cyber Diplomacy

In September 2020, we reported on State's plans at that time to establish a cyber bureau.[3] We found that State had not involved other federal agencies that contribute to international cyber diplomacy in the development of those plans, contrary to leading practices of governmental reform. We recommended that State involve relevant federal agencies in their plans to establish a cyber bureau to obtain their views and identify potential risks. Taking our recommendation and previous work into consideration, in May and June of 2021, State met with senior officials from relevant federal agencies, including the Departments of Defense, Commerce, and Homeland Security, as well as officials from the National Security Council and the Office of the National Cyber Director. During these consultations, State obtained these agencies' views and identified risks, implementing our recommendation.

In January 2021, we published another report on State's cyber bureau proposal.[4] We found that State had not demonstrated use of data and evidence to develop its proposal. Without data and evidence, we determined State lacked assurance that its proposal would effectively set priorities and allocate appropriate resources for the bureau to achieve its intended goals. We recommended that State use data and evidence to justify its current proposal or any new proposal to establish a cyber-bureau. Because of our recommendation and previous reports, State conducted qualitative internal assessments to identify staffing and skills gaps and also conducted evidence- and data-based reviews with internal

[3] See GAO, *Cyber Diplomacy: State Has Not Involved Relevant Federal Agencies in the Development of Its Plan to Establish the Cyberspace Security and Emerging Technologies Bureau*, GAO-20-607R, (Washington, D.C.: Sept. 22, 2020).

[4] See GAO, *Cyber Diplomacy: State Should Use Data and Evidence to Justify Its Proposal for a New Bureau of Cyberspace Security and Emerging Technologies*, GAO-21-266R, (Washington, D.C.: Jan. 28, 2021).

and external stakeholders over a months-long process to develop proposals to establish the bureau. Implementing data and evidence-based reviews helped to ensure that State's final proposal will achieve its intended results.

Existing Cyber Diplomacy Strategies

State officials told us that the department does not have a single unifying strategy that directs its cyber diplomacy efforts. Instead, State uses multiple strategies, including the 2023 National Cybersecurity Strategy and the 2022-2026 State and USAID Joint Strategic Plan.[5]

The March 2023 National Cybersecurity Strategy represents the most recent, national-level strategic guidance document from the executive branch. State officials told us that they use the National Cybersecurity Strategy to direct the development and implementation of cyber diplomacy activities. The strategy comprises five pillars that highlight the need for enhanced collaboration to ensure a digital ecosystem that is defensible, resilient, and aligned with U.S. values. The National Cybersecurity Strategy's fifth pillar focuses on developing international partnerships to promote responsible state behavior and maintain an open, free, global, interoperable, reliable, and secure internet. State's cyber diplomacy activities fall under Pillar V: Forge International Partnerships to Pursue Shared Goals, which describes strategic objectives that include building coalitions, strengthening capacity, and reinforcing norms, among others. This pillar is comprised of five strategic objectives. These include objectives to build coalitions to counter threats to our digital ecosystems, strengthen international partner capacity, and expand U.S. ability to assist allies and partners. In July 2023, the White House released the National Cybersecurity Strategy Implementation Plan to provide a roadmap for coordinating action across the U.S. government. The Implementation Plan describes initiatives associated with the National Cybersecurity Strategy, identifies the responsible agency, and the associated timeline for completion. For example, the Implementation Plan identifies State as the responsible agency for seven out of twelve initiatives under Pillar V of the National Cybersecurity Strategy. These initiatives include the initiative to publish an International Cyberspace and Digital Policy Strategy, which, according to State officials, is an ongoing effort that CDP is leading.

In March 2022, State and USAID released their Joint Strategic Plan (JSP) for Fiscal Year 2022-2026. The plan lays out the vision and direction for

[5] In June 2023, State published a functional bureau strategy for CDP to outline its strategic goals and objectives and to communicate State's priority efforts for cyber diplomacy.

both organizations as well as how they will implement U.S. foreign policy and development assistance. The JSP has several strategic objectives and performance goals related to cyber issues. These include promoting a stable cyberspace, strengthening U.S and allies' cyber threat capacity, and supporting U.S. technological leadership and competitiveness. Another aim is to ensure that the U.S. continues to be on the leading edge of emerging technologies. The JSP designates CDP as a lead in some of these efforts, in coordination with other State entities such as the Bureaus of Arms Control, Verification and Compliance and Economic and Business Affairs.

State Works to Advance Cyber Interests through a Range of Diplomatic and Foreign Assistance Activities

We found that State conducts a range of diplomatic and foreign assistance activities aligned with U.S. objectives outlined in the 2023 National Cybersecurity Strategy. For this report, we define diplomatic activities as activities taking place in multilateral or bilateral fora to establish cyber norms, technical standards, or build international consensus on cyber objectives. We define foreign assistance activities as activities funded by State that support technical assistance and training on cyber- and digital related topics including capacity building, confidence building measures, and others (see table 1). State has also reported on the impact of some of these activities. For example, State has a goal of getting more countries to join the Budapest Convention to combat cybercrime. [6] Nigeria's recent accession to the Convention in 2022 was an example of the impact of State's diplomatic engagement and technical assistance efforts with this country, according to State officials and related documentation.

[6] The Budapest Convention is a multilateral treaty that addresses computer related crime. It is global in nature and opened to all countries for signature in 2001. Currently there are 68 parties to the convention.

Table 1: Examples of U.S. State Department Diplomatic and Foreign Assistance Activities Supporting 2023 National Cybersecurity Strategic Objectives

Examples of Diplomatic Activities	Examples of Foreign Assistance Activities
Strategic Objective 5.1 Build coalitions to counter threats to our digital ecosystems	
• Participating in the United Nations (UN) Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security and the Open-Ended Working Group on Developments in the Field of Information Telecommunications in the Context of International Security, two major UN- sponsored, cyber-related initiatives. • Supporting efforts associated with the Summit for Democracy Presidential Initiative for Democratic Renewal, which are policy and foreign assistance initiatives aiming to bolster democracy and defend human rights, including an initiative to advance technology for democracy. Similarly, advancing principles outlined in the Paris Call, a commitment supported by 81 states to face new threats endangering citizens and infrastructure and the Declaration for the Future of Internet, a commitment by over 60 nations to advance an open, free, global, interoperable, reliable and secure internet that supports freedom, innovation and trust. • Participating in organizations such as the U.S- EU Trade and Technology Council and International Telecommunication Union to ensure technology standards align with U.S. values and to support voluntarily shared information on international standardization activities and strategic issues. • Establishing and engaging in the Freedom Online Coalition, a group of 37 countries working to build consensus and advance internet freedom by shaping global norms through joint statements in fora such as the UN.	• Supporting the Council of Europe initiative Octopus Project to deliver training and technical assistance to help align countries' domestic cybercrime and electronic evidence legislations with the standards in the Budapest Convention and advance international cybercrime cooperation. • Conducting a workshop with experts to build coalitions and to inform partners in Latin America on how the Costa Rican blueprint for secure and trusted infrastructure can be adapted to their markets with the help of the U.S., Europe, Asia, and Costa Rica.
Strategic Objective 5.2 Strengthen international partner capacity	
• Engaging in bilateral dialogues with Ukraine to reaffirm U.S. commitment to supporting Ukraine's cyber defense.	• Partnering with the Department of Justice to support the Global Law Enforcement Network activities to strengthen international cybercrime cooperation. • Participating in Digital Connectivity Cybersecurity Partnership activities, which provide technical assistance, and training to developing countries.
Strategic Objective 5.3 Expand U.S. ability to assist allies and partners	
• Supporting and engaging in the negotiation process of the U.N. Cybercrime Convention, which, if ratified, would facilitate international cooperation to combat cybercrime.	• Supporting cyber resilience activities to strengthen cybersecurity capabilities in the Organization of American States member nations.
Strategic Objective 5.4 Build coalitions to reinforce global norms of responsible state behavior	
• Supporting and advancing principles covered in the Budapest Convention, which aims to harmonize laws, standardize evidence collection, and increase law enforcement cooperation regarding cybercrime among signatory nations. • Supporting the Copenhagen Pledge on Tech for Democracy to promote digital freedom priorities and the responsible use of technology.	• Funding cyber and international law courses through the George C. Marshall Center to educate participants and affirm cyber diplomacy norms of behavior.

Examples of Diplomatic Activities	Examples of Foreign Assistance Activities
Strategic Objective 5.5 Secure global supply chains for information, communications, and operational technology products and supplies	
• Signing a bilateral memorandum of understanding with Albania agreeing to facilitate the development of secure 4G and 5G networks, the fourth- and fifth-generation technology standard for broadband cellular networks.	• Supporting 5G security campaign for countries taking action to secure 5G or next generation telecommunications networks to increase awareness of untrusted vendors. • Engaging bilaterally with Costa Rica in support of secure 5G deployment.

Source: GAO analysis of State Department data. | GAO-23-105563

State's Diplomatic Engagement in Multilateral Fora and Agreements Aims to Promote Norms of Responsible State Behavior

State engages in multilateral fora and supports multilateral agreements to strengthen norms of responsible state behaviors, deter unacceptable state behaviors, and advance cyber policies aligned with U.S. goals. State officials told us that CDP is responsible for working with multilateral organizations, such as the UN, to fortify responsible state behaviors that member states have endorsed.

The 2021 UN Report on Advancing Responsible State Behavior in Cyberspace in the Context of International Security describes norms as reflecting the expectations of the international community and setting standards for responsible State behavior consistent with international law.[7] For example, the 2021 UN report includes a norm calling on states to cooperate in developing and applying measures, such as strengthening information and communications technology policy to increase stability and to prevent practices that may threaten international security. The report also recommends nations strengthen policies to facilitate cooperation to help prevent conflict arising from the misuse of information and communication technologies. State officials told us that establishing these cyber norms, including enforcing consequences for rule-breakers, raises the cost of bad behavior in cyberspace and deters wrongdoing.

[7] U.N. Doc. A/76/135 *Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security*. July 14, 2021. The UN Group of Governmental Experts (GGE) convened six times since 2004 and produced four consensus reports in 2010, 2013, 2015, and most recently 2021. The GGE 2015 report enumerated 11 voluntary norms of State behavior in cyberspace and the GGE 2021 report further defined the framework of adopted recommendations, norms and principles for responsible state behavior in cyberspace. The consensus report defines the framework for responsible state behavior in cyberspace and reaffirms the conclusions of prior GGE consensus reports, such as the applicability of international law in cyberspace.

State Builds Coalitions in Multilateral Fora to Strengthen Norms That Align with Cyber Objectives

State works to build coalitions of countries that share U.S. strategic objectives to (1) counter threats to the U.S. digital ecosystem and (2) reinforce global norms of responsible state behavior. For example, State rallies countries that share U.S. goals to coordinate policies that advance an open, free, global, interoperable, reliable, and secure internet. Specifically, CDP officials said the department led the worldwide delegations in producing consensus reports with the UN Group of Governmental Experts (GGE) on Advancing Responsible State Behavior in Cyberspace and the Open-Ended Working Group (OEWG) on Information Telecommunications.[8] The GGE and OEWG are the two major UN-sponsored, cyber-related initiatives that State participates in to promote U.S. interests in cyberspace. According to CDP officials, these consensus reports from the GGE and OEWG are considered the most important cyber agreements created.

Officials told us that the resulting consensus reports from the GGE and the OEWG help to advance U.S. goals related to reinforcing global norms of responsible state behavior. For example, the GGE consensus report established the applicability of international laws to cyberspace and established a framework for responsible norms of state behavior. Similarly, the OEWG reaffirmed the voluntary norms as written in the GGE and further affirmed that countries try to ensure general availability and integrity of the internet, which is also in alignment with U.S. cyber goals of advancing an open, free, global, interoperable, reliable and secure internet.

State also participates in multilateral technical standards setting bodies to help ensure technical standards are developed in a consensus based and a transparent manner. For example, State coordinates with the EU through the Trade and Technology Council (TTC) to develop a mechanism to share information about international standardization activities. CDP also engages with the TTC on critical and emerging technologies through the TTC Working Group on Information and Communications Technologies Security and Competitiveness. CDP works to coordinate with the European Commission on advocacy for

[8] The first iteration of the UN OEWG ran from 2019 to 2021 and proceeded on a parallel track to the GGE. The OEWG endorsed the norms established by the GGE and provided a more inclusive forum for countries to create and disseminate cyber norms, including developing countries. In 2020, the UN General Assembly established a new five-year OEWG on the use of information and communications technologies. The 2021-2025 OEWG mandate was to further develop rules, norms, and principles of responsible state behavior and to further study data security, confidence building measures, and capacity building while promoting common understanding of such measures, among other tasks.

trustworthy telecom suppliers and to develop shared principles for 6G.[9] State reported that these activities will reinforce transparent, private sector led, consensus-based approaches to standardizing technology requirements.

State officials told us the election of a U.S. person to the Secretary General of the International Telecommunication Union (ITU) has helped to preserve the open, interoperable concept of internet and telecommunication policy as opposed to a top-down, authoritarian standards-setting approach. The election of officials from the U.S. and like-minded countries to standards setting bodies such as the ITU helps to counter threats to our digital ecosystems by working to implement reforms to make the ITU stronger, more effective and more in line with U.S. goals.

In 2011, State's Bureau of Democracy, Human Rights, and Labor (DRL) established the Freedom Online Coalition (FOC), a multilateral forum to build consensus and focus attention on internet freedom. State officials told us that the U.S. is taking over as chair of the FOC in 2023 and will leverage its diplomatic networks to advance U.S. goals and initiatives. DRL officials stated that FOC has assembled a united front on resolutions and developed language for use in other fora such as the UN. Officials from CDP told us that they collaborate with DRL on relevant issue areas and may provide support by contributing subject matter expertise on specific work. For example, State led negotiations on the adoption of a FOC joint statement condemning Iran's internet shutdowns during widespread protests in fall 2022. By holding nation states accountable for their behavior and imposing consequences for their actions, State's efforts align with the strategic objective to reinforce norms of responsible state behavior.

State Supports Multilateral Agreements to Establish or Reinforce Norms of Responsible Behavior in Cyberspace

State uses multilateral agreements to advance principals, norms, and strategic objectives by working with countries that share U.S. goals and with industries, academia, and civil society. State reports that its participation in negotiations help to shape the scope, content, and effect of multilateral agreements. For example, State's Bureau of International Narcotics and Law Enforcement Affairs (INL) reported that negotiating

[9] 6G is a wireless communication network that will succeed 5G and is expected to launch in 2030. 6G will have enhanced scalability, greater use of the radio spectrum and dynamic access to different connection types compared to 5G. This will enable greater reliability and reduce drops in connection which is critical to support advanced technologies such as drones and robots.

aspects of the UN cybercrime treaty, which is still ongoing, protected consensus-based decision-making and may help drive the adoption of global norms and standards that are in line with U.S. practices.

According to State officials, State leads the international community in accepting and affirming a collective initiative among countries in the UN. Developed over the past decade, this initiative is referred to as “The Framework for Responsible State Behavior in Cyberspace” (the Framework). The Framework is a set of cyber norms established in the UN GGE and reaffirmed in the OEWG consensus reports. The Framework consists of three pillars: international law; voluntary norms establishing what states should and should not do in the digital realm; and confidence building measures strengthening transparency, predictability, and stability. These pillars align with strategic objectives to reinforce global norms of responsible state behavior and to strengthen international partner capacity. State told us it plans to continue to help member countries understand and implement the Framework and that supporting the Framework remains a key priority.

State also conducts activities to promote countries’ accession to the Council of Europe’s Budapest Convention on Cybercrime. The convention aims to harmonize laws, standardize evidence collection, and increase cooperation among signatory nations. These concepts align with the strategic objective to reinforce global norms by holding signatory countries to the standards described in the convention. State/INL provides technical and other assistance, such as funding for the Council of Europe Cybercrime office, which assists developing countries in joining the treaty. State officials said that even if a country does not join the treaty, State still urges countries to commit to enact legislation in line with the provisions of the Convention. State tracks the number of signatories to treaties as one of the metrics to assess progress in cyber diplomacy. State/INL officials said that Nigeria’s recent accession to the Convention in 2022 was an example of the impact of INL’s diplomatic engagement and technical assistance efforts. As the Convention is not near universal ratification, State officials told us that any country’s decision to accede is significant.

In December 2019, the UN voted to establish an ad hoc committee of experts to negotiate a cybercrime treaty.[10] State/INL is leading the U.S. interagency effort along with experts in cybercrime policy, technology,

[10] A/Res/74/247 (Dec. 27, 2019).

and law enforcement from other U.S. agencies to engage with and influence the negotiations. The UN committee responsible for coordinating the negotiation process aims to build a consensus-based document and plans on finalizing language by early 2024. Efforts to establish a cybercrime treaty align with strategic objectives to expand U.S. ability to assist allies and partners and to reinforce global norms of responsible state behavior. State officials reported that their negotiation efforts prioritize protecting consensus based decision-making and help drive the adoption of global norms in line with U.S. interests and practices.

State participated in various initiatives, such as the 2018 Paris Call and the 2022 Declaration for the Future of the Internet, to advance U.S. cyber objectives. The Paris Call is comprised of nine principles to secure cyberspace that signatories commit to supporting and working together to adopt responsible behaviors in cyberspace including states, private sector partners, and civil societies. According to State, the Declaration for the Future of Internet is a political commitment among over 60 nations to affirm and commit signatories to an internet that is open, fosters competition, privacy and respect for human rights. State officials told us that activities in support of these initiatives reinforce U.S. commitment to the Framework and enhance global visibility and partnerships by aligning international positions and coordinating statements and diplomatic efforts to advance U.S. cyber objectives for an open, free, global, interoperable, reliable, and secure internet. State officials reported that the Department has been key in drafting and seeking international partner affirmation of the Declaration for the Future of the Internet. Officials also said that this initiative builds like-minded international support behind these principles and serves as a platform to advance U.S. goals.

Similarly, State supports the Summit for Democracy and the associated Presidential Initiative for Democratic Renewal[11], which focuses on strengthening democracy, defending against authoritarianism, fighting corruption, and promoting human rights. For example, in support of the Presidential Initiative's commitment to incentivize innovation in

[11]Summit for Democracy was a set of virtual summits hosted by the U.S. aiming to defend against authoritarianism, fight corruption, and advance respect for human rights. The White House held the first Summit in December 2021 and the second in March 2023. During the first Summit for Democracy, the White House announced the Presidential Initiative for Democratic Renewal. This initiative is comprised of policy and foreign assistance initiatives that support democracy and defend human rights globally by expanding efforts to sustain and grow democratic resilience with like-minded governmental and non-governmental partners.

technologies that advantage democratic values and governance, State co-hosted an event in December 2022 to encourage innovators to develop technologies in support of democracy.

State Engages Bilaterally to Advance U.S. Aligned Cyber Norms and Policies

State also maintains a number of ongoing bilateral activities to promote U.S. interests and support global consensus in cyberspace. State officials told us that CDP facilitates bilateral diplomacy efforts to achieve desired outcomes through activities such as interagency whole-of-government cyber dialogues, which involve communication with partner nations to discuss common interests. According to State officials, such engagement encourages global coordination on a collective strategy to achieve common policy outcomes. For example, in 2022, State worked with Denmark to advance the Copenhagen Pledge on Tech for Democracy (the Pledge) that counters digital authoritarianism across the globe and advances digital freedom. Following the initial bilateral effort, the Pledge enlisted signatories consisting of civil society organizations, private sector entities, and governments from over 100 countries, advancing goals and values endorsed by the U.S. related to the responsible use of technology. These efforts align with the strategic objective to build coalitions to counter threats to our digital ecosystems such as digital authoritarianism.

In June 2021, State established a memorandum of understanding between the U.S. and Albania agreeing to strengthen cooperation, facilitate the development of secure 4G and 5G networks, and to protect those networks from adversaries. The memorandum stated that using 5G networks developed by untrusted vendors could negatively impact interoperability and intelligence sharing opportunities and encouraged avoiding untrusted information and communications technologies in existing networks. The Secretary of State stated that the partnership set a strong example for the region on the importance of working with trusted vendors on sensitive technology. This effort aligns with the strategic objective to secure global supply chains for information, communications and operational technology products and services by encouraging a shift to trusted vendors for 5G networks to prevent undue risks to U.S. national security from technology that may be subject to influence from adversarial governments.

In June 2023, State led the U.S.-Ukraine Cyber Dialogue, which is an annual discussion on cyber policy issues. During the dialogue, State officials reaffirmed their commitment to supporting Ukrainians cyber defense and strengthening Ukraine’s capacity to detect, deter, and respond to cyber incidents and threats. As part of this commitment to supporting Ukraine, State announced $37 million in cyber assistance to

Ukraine. These efforts align with the strategic objective to strengthen international partner capacity.

Foreign Assistance Activities Aim to Strengthen Cooperation and Build Cyber Resilience with Training and Technical Assistance

State provides foreign assistance, such as training and technical assistance, to strengthen partner capacity and promote established cyber norms. State officials told us that CDP leads efforts to deliver pertinent programming to partner nations to help achieve US cyber policy objectives, such as reinforcing behavior consistent with the Framework or helping partner nations understand cyber norms. State also provides funding to support technical assistance activities that promote cybersecurity best practices aligned with U.S. cyber objectives. For example, State funded a series of training courses on cybersecurity capacity building and international law in partnership with the George C. Marshall Center, a German-American institution for security and defense education that promotes understanding among partner nations. State invited foreign experts to the center to educate and expose them to concepts such as the Framework, norms on peace, and cyber attribution. The training courses covered cybersecurity issues and exposed participants to skills and best practices to address complex technical and policy topics.

In May 2021, the center hosted 39 cybersecurity leaders from the national governments of 17 countries for its first course on how to collectively attribute a perpetrator of malicious cyber activities (see fig. 1). State officials told us collective attribution helps reduce the likelihood of tit-for-tat retaliation and bolsters the integrity of the allegations, reducing the credibility of denials from accused nations. State officials reported the course was intended to strengthen foreign partner's capacity to respond cooperatively to cyber threats by increasing understanding of public attribution as a policy tool and highlighted the importance of attributing malevolent cyber activities to hold actors accountable. The course, and State's ongoing training efforts, aligns with the strategic objective to strengthen international partner capacity related to cyberspace.

Figure 1: State Department Cyber Diplomacy Training Announcement for Global Cyber Security Leaders on Cyber Attribution at the George Marshall Center

Training on the Basics of
PUBLIC ATTRIBUTION FOR POLICYMAKERS
17 - 21 May 2021
PCSS
PROGRAM ON CYBER SECURITY STUDIES
ATTRIBUTION
WARNING
NODE 04
NODE 05
WARNING
BLOCK 01

Source: Department of State. | GAO-24-105563

In partnership with DOJ, State/INL supports efforts to combat cybercrime and intellectual property theft with training and technical assistance through funding the U.S. Transnational High-Tech Crime Global Law Enforcement Network (GLEN). GLEN delivers training and technical assistance to foreign law enforcement and judicial partners to combat intellectual property and cybercrime activity; builds skills in the collection and use of electronic evidence to combat all types of crime, including transnational organized crime; and delivers targeted assistance to facilitate immediate help and encourage long term institutional change. State officials reported that technical assistance provided through GLEN strengthens international cooperation and delivers cybercrime capacity building to foreign justice officials for use in the field. For example, State reported that a portion of the funding in support of GLEN facilitated the expansion of regional cryptocurrency working groups to assist with countering ransomware threats. As we have previously reported, State and DOJ conduct a variety of activities to build foreign nations' capacity to combat cybercrime including providing training, such as regional workshops to foreign law enforcement partners through GLEN.[12]

[12] See GAO, *Global Cybercrime: Federal Agency Efforts to Address International Partners' Capacity to Combat Crime*, GAO-23-104768, (Washington, D.C.: Mar. 1, 2023).

State/INL officials also reported that technical assistance promotes a rule of law-based approach to combating cybercrime and emphasizes the value of existing cybercrime instruments such as the Budapest Convention. From 2007 to 2019, the number of International Computer Hacking and Intellectual Property (ICHIP) attorney advisors, a component of GLEN, increased from one to 12.[13] Through GLEN, ICHIP attorney advisors can provide training and technical assistance via training workshops, legislative reviews, and skills development among other forms of assistance. Deploying ICHIP attorney advisors can help to strengthen cooperation and coordination with partner nations. State officials also said GLEN helps to strengthen relationships with enforcement counterparts and reinforces the advancement of international cybercrime cooperation and enforcement. These activities align with the strategic objectives to strengthen international partner capacity and to build coalitions to counter threats by building law enforcement capacity and effectiveness through training and assistance from technical advisors and advancing international cybercrime cooperation.[14]

State/INL contributes funding to the Octopus Project, a Council of Europe cybercrime program established in 2014 to strengthen developing countries' laws to be consistent with the Budapest Cybercrime Convention. This initiative is ongoing and delivers training and technical assistance to developing countries to enable them to request accession to the Convention. State officials said that providing such foreign assistance helps countries adopt necessary infrastructure protections. This initiative aligns with the strategic objective to strengthen international partner capacity by providing developing countries policy advice, training, and technical assistance to enable them to bring their laws to standards required to join the Convention. State reported that while supporting this

[13] The ICHIP program deploys attorneys overseas to assess the capacity of law enforcement authorities, develop and deliver training, build, and strengthen institutions, and monitor regional trends.

[14] In March 2023, we reported on efforts that the Departments of State, Justice, and Homeland Security are undertaking to build international partner capacity to combat cybercrime and key challenges to these efforts. These collaborative activities included sharing information with foreign partners on current threats and providing cyber training to foreign law enforcement, among many other activities. However, as the lead agency responsible for foreign assistance, State had not fully evaluated whether these activities have been effective in helping foreign nations combat cybercrime. We recommended that it do so. State agreed with this recommendation, and identified actions that it will take in the future. Our recommendation will remain open until State completes these actions. For more information, see GAO-23-104768.

program, the number of parties to the Convention increased from 40 to 68.

State works to support strengthening cyber capacity building through efforts to improve overall cyber resilience in Organization of American States (OAS) member states and by enhancing cooperation and coordination among relevant stakeholders. State officials told us that as the OAS working group chair on cybersecurity issues, CDP works with OAS to build regional dialogue on cybersecurity measures. For example, State officials told us they are the current chair of the OAS Confidence Measure working group. State and OAS then work with member states on implementing practical measures in accordance with existing agreements on cyber norms, according to State officials.

State also reported that they support OAS through activities such as providing funding for a capacity-building project that intends to increase access to knowledge and information on cyber threats to inform the formulation of confidence building measures. An OAS project proposal report stated that improving cyber resilience supports U.S. cyber objectives of building capacity by advancing key tenets of an open, free, global, interoperable, reliable, and secure internet.[15] OAS reported that U.S. assistance will help strengthen cyber capacity of regional partners and assist in building consensus on cyber issues.

Led by State and co-chaired by USAID, the Digital Connectivity Cybersecurity Partnership (DCCP) is a global, interagency, whole of government initiative to promote an open, interoperable, secure, and reliable internet. State provides funding for DCCP activities and DCCP aligns with the strategic objective to strengthen international partner capacity. DCCP works to counter threats to our digital ecosystem by (1) promoting inclusive, multi-stakeholder models of internet governance, (2) building connections by promoting investments in resilient information and communications technology infrastructure, and (3) enhancing cybersecurity by facilitating adoption and implementation of cybersecurity best practices.

DCCP also manages foreign assistance activities related to strengthening international partner's information and communications technology ecosystems, which is supported by a portion of the International

[15] Organization of American States Inter-American Committee Against Terrorism Cybersecurity Program. *United States support to continue strengthening cybersecurity capabilities in OAS Member States*. August 2021.

Technology Security and Innovation Fund, established by the Creating Helpful Incentives to Produce Semiconductors (CHIPS) Act of 2022.[16] As a recipient of these funds, CDP was able to substantially elevate cyber and digital focused foreign assistance in support of like-minded partners, according to CDP officials.

According to State officials, the programs in this partnership constitute a significant portion of cyber-related foreign assistance activities supported by State. USAID officials said that the Digital Asia Accelerator (DAA) program running from September 2019 to September 2024 is a particularly successful DCCP activity that leveraged the know-how of U.S. technology companies and the expertise and contextual knowledge of local organizations. The DAA was designed in support of the goal of advancing open, interoperable, reliable, and secure internet and to advance cybersecurity by improving digital safety practices, increasing the capacity for stakeholders in Southeast Asia to engage on digital economy policy issues, and developing different modes of programming tools to reach key audiences. Officials reported that 24,500 individuals completed training on digital skills through programming activities and the program provided access to information on digital safety to over 2.3 million people.

State also provides foreign assistance on a bilateral basis. For example, State provided technical advice, guidance, and engagement in support of Costa Rica's digital infrastructure and equipment upgrade for 5G deployment. State officials said that they expect that the resources and engagement will result in the successful execution of contracts with trusted telecommunications vendors. This effort aligns with the strategic objective to secure global supply chains for information, communications, and operational technology products and supplies.

In addition, in March 2023, State announced a $25 million cybersecurity assistance package to strengthen Costa Rica's cyber defense against threats from malicious actors following a year of repeated ransomware attacks on Costa Rica's government networks that impacted critical services such as health care, tax collection, and customs, and resulted in a national emergency. This funding aims to establish and equip a

[16] Pub. L. No. 117.167, Div. A, § 102(c), 136 Stat 1375 (Aug. 2022). This fund provides the Department of State with $500 million—$100 million per year over five years, starting in Fiscal Year 2023—to promote the development and adoption of secure and trustworthy telecommunications networks and ensure semiconductor supply chain security and diversification.

centralized Security Operations Center to monitor, prevent, detect, investigate, and respond to cyber threats and provide immediate support for cybersecurity training operations, cybersecurity tools, and longer-term capacity building. This assistance aligns with the strategic objective to expand U.S. ability to assist allies and partners by supporting partner nations' ability to investigate, respond to, and recover from cyberattacks.

State officials told us that they also work with other agencies through formal interagency agreements (IAA) in addition to informal coordination efforts to leverage expertise, broaden insights, and develop a whole of government approach to executing foreign assistance activities. CDP is currently managing 11 cyber-related IAAs with agencies including the Departments of Commerce and the Interior, DOD, DHS, and the Federal Communications Commission.[17] These agreements focus on promoting capacity building, technical assistance, and training (see table 2). For example, an IAA with Department of Commerce is focused on supporting State's global 5G security campaign to increase awareness of untrusted vendors by providing guidance, expertise, and technical assistance. Specifically, Commerce would provide best practice guides and bilateral technical assistance on a range of 5G security related topics and national security legislation. These activities align with the strategic objective to secure the global supply chain for information, communication, and operational technology products and supplies and to advocate for an open, interoperable, and secure internet by promoting 5G security.

[17] In addition to the interagency agreements managed by the Bureau of Cyberspace and Digital Policy, other bureaus may manage interagency agreements related to cyber activities.

Table 2: List of Cyber Diplomacy Related Interagency Agreements Managed by U.S. State Department Bureau of Cyberspace and Digital Policy

Agency	Program Description	Estimated Funding Amount	Period of Performance
Department of Commerce (Commerce)	Engages civilian foreign governments, foreign industry partners, and other foreign civilian stakeholders as appropriate, on the application and implementation of U.S. developed cybersecurity best practices and frameworks. The goal of this program is to develop and support partner nations' capacity and capabilities to build their national and regional cybersecurity through the consideration of and potential sustainable adoption of US aligned frameworks and guidelines	$20,000,000	09/23/2020–9/30/2025
Commerce	Facilitates the development of a software tool to help create a consistent and comprehensive approach enabling data flows across the globe. This effort also will work to support the adoption of interoperable approaches to protecting privacy.	$1,250,000	09/30/2019–09/30/2023
Commerce	Provides legal and regulatory advising in support of State's 5G security campaign. Commerce will support State in advising and providing information on best practices, national security legislations, and measures to prohibit untrusted vendors in their telecommunications networks.	$2,250,000	09/24/2020–09/30/2023
Commerce	Provides guidance, expertise, analysis and technical assistance in support of State's advocacy efforts for security internet and information and communications technology development in the western hemisphere affairs region.	$1,645,000	09/24/2020–09/30/2023
Department of Defense (DOD)	Improves the ability of national governments and related regional stakeholders to address cybersecurity threats to civilian networks and internet telecommunication infrastructure.	$50,000,000	10/01/2015–08/30/2025
DOD	Provides senior and mid-level cybersecurity strategy, policy and awareness education for partner nation governmental participants through the conduct of in-resident courses and outreach events, such as workshops and seminars to improve understanding of current and emerging cyber threats and how to develop mitigating strategy and policy solutions and influence legislative and regulatory improvement.	$20,000,000	10/01/2017–09/30/2025
Department of Homeland Security (DHS)- Cybersecurity and Infrastructure Security Agency (CISA)	Provides training and resources to enhance industrial control systems cybersecurity capabilities. The capabilities will focus on the ability to defend existing networks, provide earlier detection of cyber threats and more effectively analyze cyber events.	$1,400,000	09/30/2020–09/30/2023
DHS - CISA	Builds critical infrastructure protection capacity for targeted countries and support efforts to address cybersecurity issues in the international environment as well as support efforts of allies and likeminded nations.	$500,000	09/30/2021–09/29/2026

Agency	Program Description	Estimated Funding Amount	Period of Performance
Federal Communications Commission (FCC)	Supports travel for FCC employees to participate in meetings, technical consultations conferences, trainings, and other activities that directly support DCCP objectives and the 5G campaign.	$75,000	07/21/2020–09/30/2023
Department of Interior	Contractor will ensure DCCP monitoring and evaluation framework is compliant with the State Department's program design policies such as having a project schedule and a project charter to define the goal, scope, and deliverables.	$1,047,468	09/30/2021–09/30/2022
United States Agency for International Development	Addresses and improves cybersecurity capacity building needs globally. The program aims to develop and support partner nations' capacity and capabilities in cyberspace and digital policy.	$3,100,000	10/01/2022–09/30/2024

Source: Interagency Agreements from Department of State. | GAO-23-105563

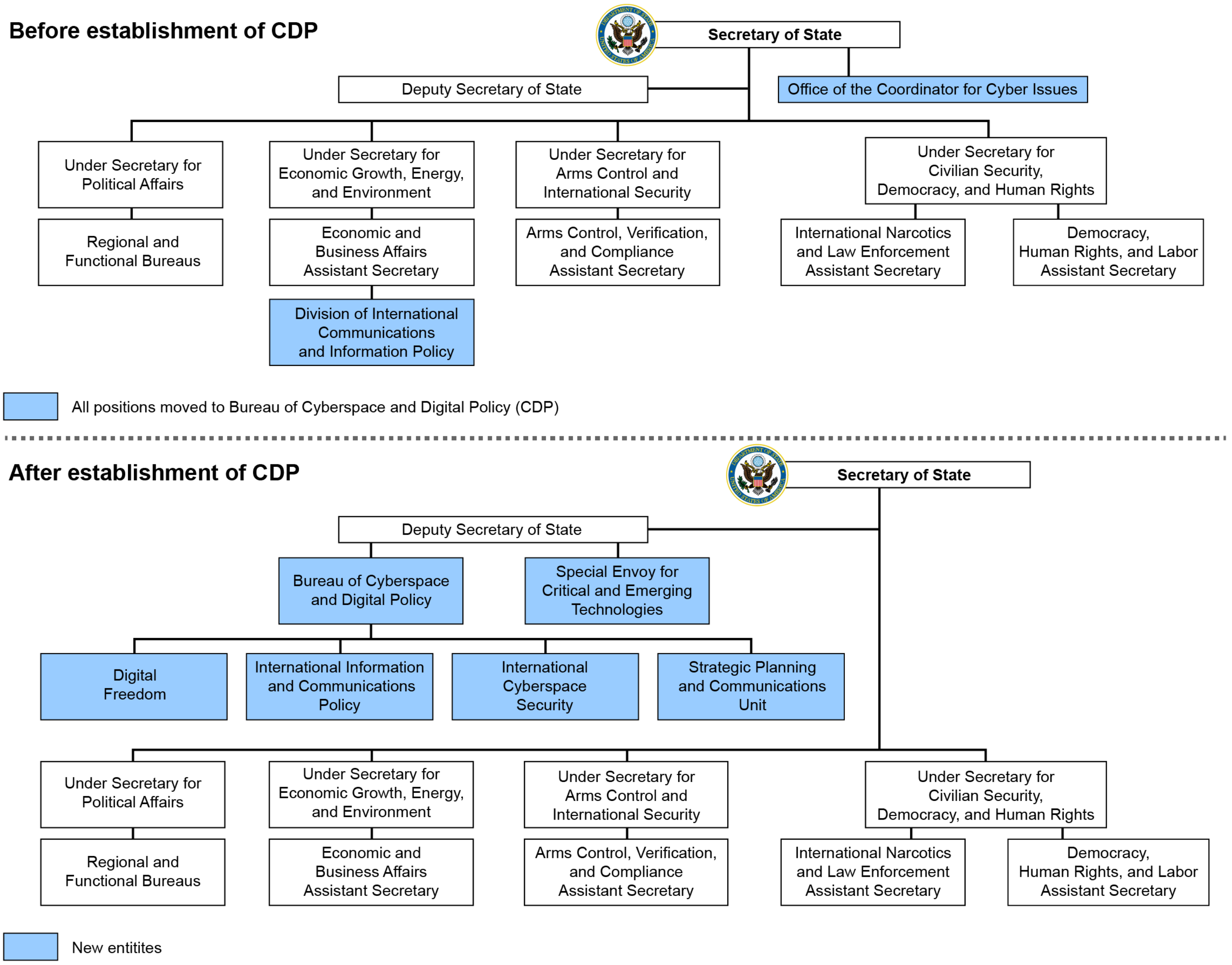
Note: This table only represents interagency agreements managed by the Bureau of Cyberspace and Digital Policy. Other bureaus may also manage interagency agreements related to cyber activities, however they are not reported here.

State's Reform Effort Has Helped to Elevate Cyber Diplomacy Goals and Aligned with Leading Practices

State Established a New Bureau to Prioritize Cyber Diplomacy

In April 2022, State established a new Bureau of Cyberspace and Digital Policy (CDP) with a mission to address national security challenges, economic opportunities, and implications to U.S. values associated with cyberspace, digital technologies, and digital policy. State created CDP, headed by a Senate-confirmed Ambassador-at-Large, to elevate cyberspace as an organizing concept for U.S. diplomacy by consolidating efforts and leadership of cyberspace-related activities into a single unit. Previously, State distributed responsibility for cyber issues between the Office of the Coordinator for Cyber Issues (S/CCI) and other entities, according to officials (see fig. 2).

Figure 2: Elements of State Department Organization Chart Reflecting Consolidation of Cyber Diplomacy Structure


Before establishment of CDP
Secretary of State
Deputy Secretary of State
Office of the Coordinator for Cyber Issues
Under Secretary for Political Affairs
Under Secretary for Economic Growth, Energy, and Environment
Under Secretary for Arms Control and International Security
Under Secretary for Civilian Security, Democracy, and Human Rights
Regional and Functional Bureaus
Economic and Business Affairs Assistant Secretary
Arms Control, Verification, and Compliance Assistant Secretary
International Narcotics and Law Enforcement Assistant Secretary
Democracy, Human Rights, and Labor Assistant Secretary
Division of International Communications and Information Policy
🟦 All positions moved to Bureau of Cyberspace and Digital Policy (CDP)
After establishment of CDP
Secretary of State
Deputy Secretary of State
Bureau of Cyberspace and Digital Policy
Special Envoy for Critical and Emerging Technologies
Digital Freedom
International Information and Communications Policy
International Cyberspace Security
Strategic Planning and Communications Unit
Under Secretary for Political Affairs
Under Secretary for Economic Growth, Energy, and Environment
Under Secretary for Arms Control and International Security
Under Secretary for Civilian Security, Democracy, and Human Rights
Regional and Functional Bureaus
Economic and Business Affairs Assistant Secretary
Arms Control, Verification, and Compliance Assistant Secretary
International Narcotics and Law Enforcement Assistant Secretary
Democracy, Human Rights, and Labor Assistant Secretary
🟦 New entitites

Source: GAO based on Department of State documentation (data); Department of State (seals). | GAO-24-105563

The U.S. Ambassador-at-Large for Cyberspace and Digital Policy has high-level duties and responsibilities associated with fulfilling strategic objectives, including serving as the principal cyberspace policy official within the senior management at State and as the advisor to the Secretary of State for cyberspace and digital issues.

The establishment of CDP as a bureau level entity with high-level leadership has highlighted the importance of cyber diplomacy, according to State officials. For example, an official told us that the creation of this ambassador level leadership and authority over cyber issues has enabled engagement with higher levels of foreign government officials and raised the U.S. profile on cyber globally. Since taking office, the Ambassador has engaged with various countries' senior leaders on advancing cyber goals. As an example, in August 2023, the Ambassador headed the U.S. delegation to the G20 Digital Economy Ministerial Meeting in Bengaluru, where he highlighted U.S. views on digital economy topics including priority areas set by India's G20 presidency; and met with technology entrepreneurs and other representatives from industry and civil society.

In addition, CDP's status as a bureau provides senior level support, resources, and involvement that did not exist before, which strengthened the stature of cyber issues within State. For example, according to the senior state officials, the creation of CDP increased awareness of and technical literacy in cyber policy issues internally, giving greater voice and legitimacy to cyber issues State Department-wide. The head of CDP told us that the session on cyber at the annual Chiefs of Mission conference in 2023, which gathers ambassadors from posts worldwide, was completely filled, highlighting the level of interest and attention the issue now commands at State. State officials also stated that organizational consolidation and new role definitions helped cut through significant bureaucracy, enabling cyber issues to take on a higher profile.

CDP contains three policy units:

- **International Cyberspace Security:** leads State efforts to promote cyberspace stability and security, including diplomatic engagement on international cyberspace security in multilateral, regional, and bilateral forums with a staff of 37.
- **International Information and Communications Policy:** works to promote competitive and secure networks, including 5G, and protect telecommunication services and infrastructure through licensing, sanctions enforcement, and supply chain security with a staff of 37.
- **Digital Freedom:** supports State work on privacy, government intervention, human rights, and civic engagement to promote global internet freedom with six staff members.

According to State officials, CDP's Strategic Planning and Communications Unit is responsible for the Bureau's strategic planning, public diplomacy, media, legislative affairs activities, and manages its foreign assistance programs via the Digital Connectivity and Cybersecurity Partnership.

CDP is funded from State's primary operating account Diplomatic Programs, and annually requests funds from the Diplomatic Policy and Support category, which supports the operational programs of the functional bureaus. In Fiscal Year 2022, State allocated $18 million, for CDP to support the bureau and 92 positions. In subsequent requests, State requested additional increases to fund new positions, and in Fiscal Year 2023, allocated $21 million for CDP.

In January 2023, after the establishment of the Bureau, State also stood up the Office of the Special Envoy for Critical and Emerging Technology within the Office of the Secretary (S/TECH) to integrate critical and emerging technologies into U.S. foreign policy and diplomacy. S/TECH leads foreign policy and diplomacy on critical and emerging technologies and focuses on artificial intelligence, biotechnology, and quantum information technology. Both CDP and S/TECH report to the Deputy Secretary, with S/TECH reporting through CDP's Ambassador-at-Large.

State's New Bureau Is Addressing Challenges as It Works to Achieve Strategic Objectives

According to State officials, CDP is addressing challenges as it pursues strategic objectives, including clarifying roles and hiring staff. State officials said that although responsibilities for cyber issues are defined under the new structure, roles remain deliberately shared and complementary department-wide, so clarification is an ongoing challenge. In addition, State officials told us that since cyber issues may be relevant to almost any aspect of diplomacy, communication within State to ensure awareness and visibility of issues so expertise is fully utilized is an important, related challenge. For example, CDP's Digital Freedom unit and the Bureau of Democracy, Human Rights, and Labor (DRL) cover similar areas such as free speech on and fair access to the internet. CDP's role is to contribute expertise on tech policy, to collaborate with other State units to develop complementary positions on topics, and to engage with partner countries on statements and other activities, whereas DRL's role is to advance internet freedom through bilateral and multilateral diplomacy and by funding civil society-led projects.

According to State officials, the lack of a globally agreed definition for cyber diplomacy and the diverse ways that foreign governments, multilateral actors, civil society and the private sector organize themselves on cyber topics contributes to the challenges that they face in identifying roles and responsibilities for some cyber issues. State officials said that structured and unstructured mechanisms, such as regular meetings and informal conversations, facilitate communication between CDP and other bureaus and offices regarding these issues. Further, when multiple bureaus are involved in an issue, officials clarify roles on an ad hoc basis. This approach is helping to avoid conflicts and communication breakdowns, according to officials we spoke with in bureaus at State.

CDP also works to clarify State's role in the U.S. government-wide interagency process. CDP works to ensure State maintains the lead in cyber diplomacy and coordinates action with other U.S. agencies. For example, State recently led a delegation of officials from U.S. Cyber Command, the Office of the National Cyber Director, and the Cybersecurity and Infrastructure Security Agency that met with Ukrainian Deputy Ministers and announced $37 million in non-military cyber assistance for Ukraine, as mentioned above.

State officials told us that CDP is currently staffed and fully operational but needs to train existing staff and to hire more people to meet its growth plans. To address current skill gaps, CDP implemented a knowledge sharing program on areas of expertise including international cybersecurity partnership initiatives, information and communications policy work, digital freedom policy work, interagency coordination, foreign assistance work, and bilateral/multilateral engagements. CDP also established a Cyber and Digital Policy Officer course at State's Foreign Service Institute and is working to provide the content on-demand virtually to make it easily accessible and available to staff worldwide. The CDP head told us that his goal is to ensure there is a trained Cyber and Digital Policy Officer at every embassy by the end of 2024. State is also establishing a mechanism to identify cyber skills department-wide, so that staff can be matched to jobs and provided with incentives. In addition, State added fluency in cyber topics as selection criteria for ambassadors. Further, State launched an annual "Achievement in Tech Diplomacy" award to highlight the importance of cyber diplomacy within the department. To address hiring needs, CDP also is implementing and exploring additional to expedite the process and working to develop partnerships with industry, academia, and other agencies to create a talent pipeline.

State Followed Relevant Leading Reform Practices When Establishing Its New Cyber Bureau

Prior GAO work on agency reform efforts identified leading reform practices for federal government organizational changes and efforts to streamline and improve the efficiency and effectiveness of operations.[18] Among the set of general practices, we focused on those relevant and applicable to State's implementation of the reform effort.

In creating CDP, State addressed eight leading reform practices (see table 3).

Table 3: The Department of State Addressed Relevant Leading Reform Practices in Establishing the Bureau of Cyberspace and Digital Policy

Reform Practice and Questions	GAO Assessment
Leadership. Has the agency designated a leader or leaders to be responsible for the implementation of the proposed reforms?	Addressed
Accountability. How will the agency hold the leader or leaders accountable for successful implementation of the reforms?	Addressed
Implementation Team. Has the agency established a dedicated implementation team that has the capacity, including staffing, resources, and change management, to manage the reform process?	Addressed
Implementation Plan. What implementation goals and a timeline have been set to build momentum and show progress for the reforms? In other words, has the agency developed an implementation plan with key milestones and deliverables to track implementation progress?	Addressed
Employee Engagement. How does the agency plan to sustain and strengthen employee engagement during and after the reforms?	Addressed
Diversity. How specifically is the agency planning to manage diversity and ensure an inclusive work environment in its reforms, or as it considers workforce reductions?	Addressed
Strategic workforce Plan. To what extent has the agency conducted strategic workforce planning to determine whether it will have the needed resources and capacity, including the skills and competencies, in place for the proposed reforms or reorganization?	Addressed
Recruitment. To what extent have the reforms included important practices for effective recruitment and hiring such as customized strategies to recruit highly specialized and hard-to-fill positions?	Addressed

Source: GAO analysis of State Department data. | GAO-23-105563

Further detail on State addressing the practices is provided below:

Leadership: State designated leaders for the reform effort including the Ambassador-At-Large, Principal Deputy Assistant Secretary, and Executive Director.

Accountability: Similar to other bureaus within State, CDP will be held accountable through its performance plan process, which includes monitoring and reporting performance goals established by supervisors in

[18] GAO-18-427.

collaboration with each employee. To support this process, CDP developed a Functional Bureau Strategy (FBS), which identifies goals, objectives, and sub-objectives related to advancing cyber policies globally and elevating digital foreign policy within the U.S. government. CDP developed a strategy implementation plan that includes tracking progress using performance indicators and milestones on a quarterly bases and through quarterly Senior Leadership Strategy Review discussions, according to officials and related documentation. CDP will report on performance during State's annual Statement of Assurance process in a manner similar to how units that played a role in cyber diplomacy before CDP existed reported performance.

Implementation Team: State created an implementation team with working groups with expertise and competencies dedicated to addressing capacity staffing, resources, and change management. For example, the Communications and Change Management Working Group was responsible for engaging with those directly affected by the creation of CDP, with staff State-wide, and with external audiences. State's most senior public affairs officials, staff from the former Office of the Coordinator for Cyber Issues, and staff from the former Division for Information and Communications Policy with experience in process management and communications led the group.

Implementation Plan: State identified a set of required tasks before and during the reform effort, and developed milestones to track progress, addressing elements of an implementation plan. Specifically, CDP created a pre-launch plan with tasks, and during the reform effort, developed an assessment that identifies objectives, sub-objectives and relevant units involved in each, with a heading to track desired end state. In September 2022, CDP conducted a strategy review and produced objectives and milestones aligned to CDP goals. In addition, CDP will use the FBS to track progress, according to officials.

Employee Engagement: CDP conducted an off-site and solicited employee feedback on alignment with vision, values, and goals shortly after its creation. CDP also held monthly Ambassador "Town Halls," weekly team calls, a virtual "Lunch and Learn" series, and other engagement activities. CDP continues to explore additional communication tools, various working groups, and other approaches including co-located open concept space accommodations with shared workstations to sustain employee engagement.

Diversity: In coordination with the Department-wide Diversity, Equity, Inclusion, and Accessibility (DEIA) Strategic Plan, CDP established a DEIA council that will review and align DEIA bureau strategies, with an emphasis on hiring efforts to help ensure the use of best practices.

Strategic Workforce Plan: GAO's prior work describes a strategic approach to workforce planning.[19] State/CDP addressed strategic workforce planning, as described below.

- In the CDP Training and Field Support Strategy (TFSS), a document on closing the gap in cyberspace proficiency at State, CDP identifies the critical skills and competencies that will be needed to achieve current and future goals. For example, one skill at the basic level is possession of a conception of cyber and digital policy terminology and another is understanding how cyber and digital policy issues impact U.S. security, economic competitiveness, and values.
- The TFSS outlines strategies tailored to address skills gaps, including approaches such as delivering an in-person formal training course, creating a companion virtual course, and conducting regional workshops.
- The TFSS identifies resources, including funding and staff, for building the internal capability needed to support workforce planning strategies.
- According to CDP officials, to monitor and evaluate progress toward closing skills gaps, CDP conducted a baseline survey on proficiency levels in November 2022, and will be conducting the survey on a regular basis to measure changes and will make adjustments accordingly. CDP also monitors skill gaps through post-training surveys, conducted with the Foreign Service Institute, State's training unit, that provide another set of quantitative and qualitative data points.

Recruitment: State used special hiring authorities, such as Direct Hire Authority, as well as special programs, such as the Foreign Affairs Information Technology Fellowship Program to meet mission priorities. As mentioned above, CDP is exploring additional special hiring mechanisms to expedite the process and working to develop partnerships with industry, academia, and other agencies to create a talent pipeline.

[19] See GAO, High-Risk Series: An Update, p. 51, GAO-13-283, (Washington, D.C.: Feb. 2013).

Agency Comments

We provided a draft of this report to State, USAID, DOD, and DHS for review and comment. USAID provided written comments that are reprinted in appendix II. State and DHS provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of State, the USAID Administrator, the Secretary of Defense, and the Secretary of Homeland Security. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-4409 or LoveGrayerL@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

Latesha Love-Grayer

Latesha Love-Grayer
Director, International Affairs and Trade

List of Addressees

The Honorable Benjamin Cardin
Chairman
The Honorable James E. Risch
Ranking Member
Committee on Foreign Relations
United States Senate

The Honorable Michael McCaul
Chairman
The Honorable Gregory Meeks
Ranking Member
Committee on Foreign Affairs
House of Representatives

The Honorable Robert Menendez
United States Senate

Appendix I: Objectives, Scope, and Methodology

This report examines (1) activities State is undertaking to advance U.S. interests regarding cyberspace, including the use of international agreements and fora, and what has been reported about their impact; and (2) the extent to which organizational changes have helped position or presented challenges for State to achieve its cyber diplomacy goals.

To identify activities State is undertaking to advance to advance U.S. interests regarding cyberspace, we reviewed documentation on State cyber diplomacy activities from 2017 to present and focused on ongoing and recent activities from 2020 through 2023. While multiple agencies may conduct foreign assistance activities in support of cyber diplomatic activities, we focused our audit work on cyber diplomacy activities that State leads or provides funding for or that have a structured relationship with State, such as a reporting requirement or formal interagency agreement. We defined cyber diplomacy programs or activities as those contributing to cyber diplomacy goals identified in the 2018 National Cyber Strategy Pillar III: Preserve Peace through strength or Pillar IV: Advance American Influence.

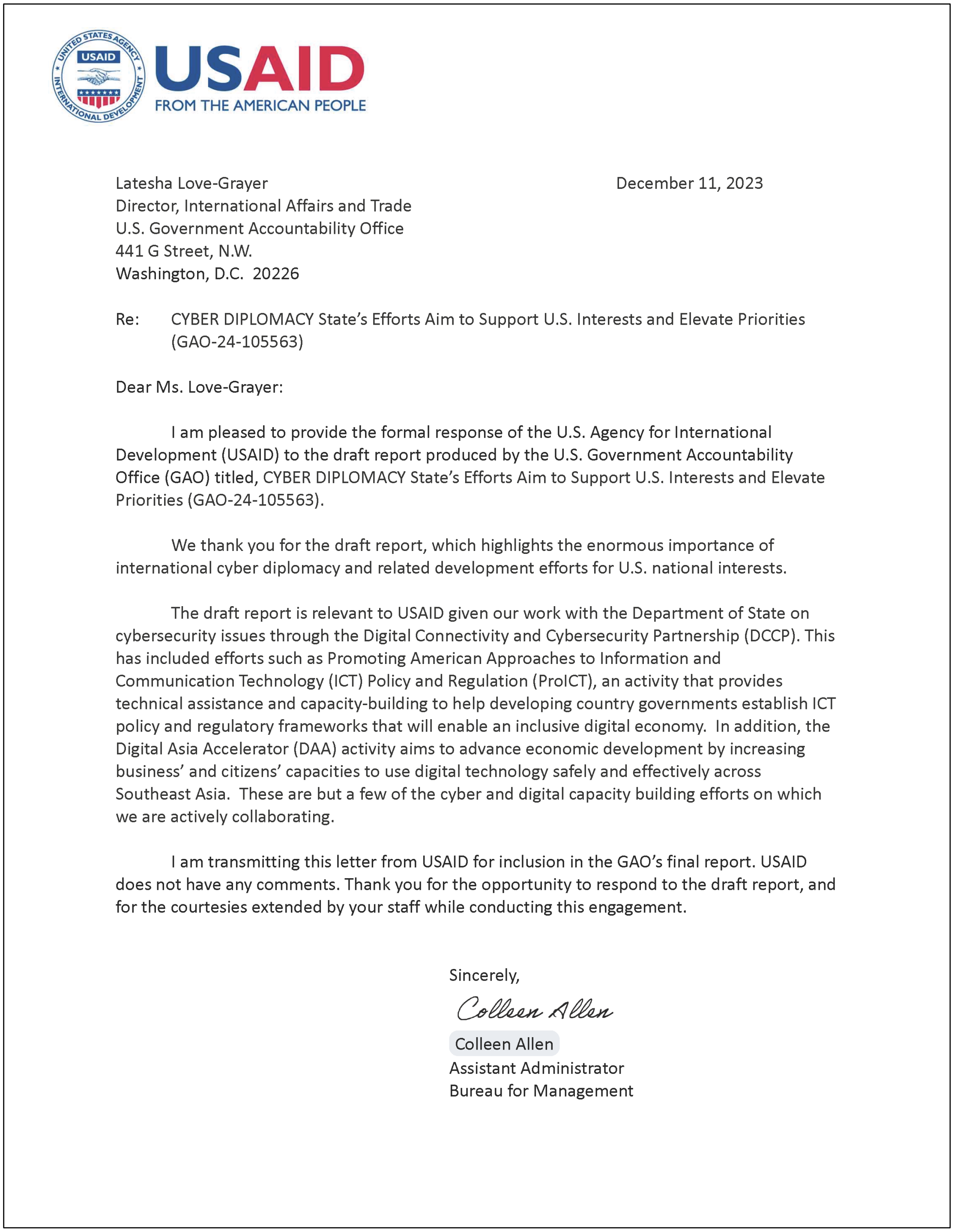
While the request for information was made prior to the release of the 2023 National Cybersecurity Strategy, we analyzed the activities and programs identified by State and other agencies to determine their alignment to the strategic objectives in the 2023 National Cybersecurity Strategy Pillar V. We selected Pillar V: Forge International Partnerships to Pursue Shared Goals because this pillar focuses on international cyber efforts. We determined that for the purposes of our report, the strategic objectives contained in the 2018 National Cyber Strategy and the 2023 National Cybersecurity Strategy captured similar themes and concepts with regard to international cyber objectives. We analyzed program documents and discussed strategic objectives and their implementation with officials from State and relevant agencies, including the United States Agency for International Development (USAID), Department of Defense (DOD), and Department of Homeland Security (DHS).

We identified a set of multilateral fora, multilateral and bilateral agreements and foreign assistance activities, to illustrate the range and impact of cyber diplomacy activities that State is supporting. We reviewed results of selected programs and spoke with State officials to determine what has been reported about impact. Some activities we reviewed began prior to the formation of the Bureau of Cyberspace and Digital Policy (CDP), but provide illustrative examples of State cyber diplomacy efforts. Further, CDP continues to support these activities; accordingly, we mention them in our report as appropriate.

To examine the extent to which organizational changes helped position or presented challenges for State to achieve its cyber diplomacy goals, we analyzed documentation of and spoke with officials about State's rationale, plans, and organizational changes. Specifically, we reviewed documents including State's implementation plan for CDP, its assessment of objectives, a strategy review, a memo related to the establishment of CDP, the Training and Field Support Strategy, and workforce plan for CDP. We also gathered information from a detailed set of questions to which State responded in writing. We also spoke with officials and representatives from non-governmental organizations about challenges and priorities and approaches to address them. We evaluated the organizational changes by assessing the extent to which State addressed selected government reform practices, outlined in prior GAO work. To examine the extent to which organizational changes have helped position State to achieve its cyber diplomacy goals, we assessed how State addressed applicable government reform practices to meet its goals. We determined a practice was applicable if it was relevant to and could be implemented reasonably in the context of State's organizational change.

We conducted this performance audit from November 2021 to January 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the U.S. Agency for International Development



USAID
FROM THE AMERICAN PEOPLE

Latesha Love-Grayer
Director, International Affairs and Trade
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20226

December 11, 2023

Re: CYBER DIPLOMACY State's Efforts Aim to Support U.S. Interests and Elevate Priorities (GAO-24-105563)

Dear Ms. Love-Grayer:

I am pleased to provide the formal response of the U.S. Agency for International Development (USAID) to the draft report produced by the U.S. Government Accountability Office (GAO) titled, CYBER DIPLOMACY State's Efforts Aim to Support U.S. Interests and Elevate Priorities (GAO-24-105563).

We thank you for the draft report, which highlights the enormous importance of international cyber diplomacy and related development efforts for U.S. national interests.

The draft report is relevant to USAID given our work with the Department of State on cybersecurity issues through the Digital Connectivity and Cybersecurity Partnership (DCCP). This has included efforts such as Promoting American Approaches to Information and Communication Technology (ICT) Policy and Regulation (ProICT), an activity that provides technical assistance and capacity-building to help developing country governments establish ICT policy and regulatory frameworks that will enable an inclusive digital economy. In addition, the Digital Asia Accelerator (DAA) activity aims to advance economic development by increasing business' and citizens' capacities to use digital technology safely and effectively across Southeast Asia. These are but a few of the cyber and digital capacity building efforts on which we are actively collaborating.

I am transmitting this letter from USAID for inclusion in the GAO's final report. USAID does not have any comments. Thank you for the opportunity to respond to the draft report, and for the courtesies extended by your staff while conducting this engagement.

Sincerely,

Colleen Allen

Colleen Allen
Assistant Administrator
Bureau for Management

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Latesha Love-Grayer, (202) 512-4409, LoveGrayerL@gao.gov

Staff Acknowledgements:

In addition to the contact named above, Rob Ball (Assistant Director), Marc Castellano (Analyst-in-Charge), Neil Doherty, Mark Dowling, Thomas Friend, Kush Malhotra, Donna Morgan, Andrew Stavisky, Sarah Veale, and Jina Yu made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548