U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

Accessible Version

September 22, 2020

The Honorable Eliot L. Engel
Chairman
The Honorable Michael T. McCaul
Ranking Member
Committee on Foreign Affairs
House of Representatives

CYBER DIPLOMACY: State Has Not Involved Relevant Federal Agencies in the Development of Its Plan to Establish the Cyberspace Security and Emerging Technologies Bureau

The United States and its allies are facing expanding foreign cyber threats, as international trade, communication, and critical infrastructure become increasingly dependent on cyberspace.[1] The United States also faces challenges to build consensus within international organizations on setting standards for how to govern the internet and cultivating norms for acceptable nation state behavior in cyberspace. The Department of State (State) leads U.S. government international efforts to advance the full range of U.S. interests in cyberspace, including by coordinating with other federal agencies, such as the Departments of Commerce (Commerce), Defense (DOD), Energy (DOE), Homeland Security (DHS), Justice (DOJ), and the Treasury (Treasury), to improve the cybersecurity of the nation. Specifically, in 2016, the *Department of State International Cyberspace Policy Strategy*[2] affirmed the elevation of cyberspace policy as a foreign policy imperative and the prioritization of State's efforts to mainstream cyberspace policy issues in its diplomatic activities. In 2018, pursuant to Executive Order 13800,[3] State led the development of an international engagement strategy in coordination with other federal agencies to strengthen the U.S. government cooperation with other countries and international organizations to address shared threats in cyberspace.[4]

---

[1]Cyberspace is the globally interconnected digital information and communications infrastructure. See GAO, *Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance*, GAO-10-606 (Washington, D.C.: July 2, 2010).

[2]*Department of State International Cyberspace Policy Strategy*, March 2016. Accessed October 22, 2019. https://2009-2017.state.gov/documents/organization/255732.pdf.

[3]Exec. Order 13800, 82 Fed. Reg. 22391 (May 16, 2017).

[4]Department of State, Office of the Coordinator for Cyber Issues, *Recommendations to the President on Protecting American Cyber Interests through International Engagement*, May 31, 2018. Accessed August 7, 2019.

In 2019, members of Congress introduced the Cyber Diplomacy Act of 2019,[5] which would establish a new office to lead State's international cyberspace efforts that would consolidate cross-cutting efforts on international cybersecurity, digital economy, and internet freedom, among other cyber diplomacy issues.[6] In June 2019, State notified Congress of its intent to establish a new Bureau of Cyberspace Security and Emerging Technologies (CSET) that would focus more narrowly on cyberspace security and the security aspects of emerging technologies.[7] According to State officials, Members of Congress raised objections to State's plan, which has not been implemented as of August 2020.

You asked us to review State's efforts to advance U.S. interests in cyberspace, including State's planning process for establishing a new bureau to lead its international cyber mission. This report examines the extent to which State involved other federal agencies in the development of its plan for establishing CSET. As part of our ongoing work on this topic, we are also continuing to monitor and review State's overall planning process for establishing this new bureau.

To address this objective, we reviewed U.S. strategies related to State's international cyberspace efforts and available documentation from State on its planning process for establishing the new bureau. We interviewed officials at State, Commerce, DOD, DOE, DHS, DOJ, and Treasury to discuss State's planning efforts and consultations with these agencies. To determine the extent to which State involved other agencies in the development of its plans, we assessed State's efforts against relevant key practices for agency reforms compiled in our June 2018 report on government reorganization.[8] Because this review is focused on how State involved other agencies in the development of its plans, we addressed the key practice of how and to what extent the agency has involved other stakeholders in the development of the proposed reforms to ensure the reflection of their views. These stakeholders include the agency's customers and other agencies serving similar customers or supporting similar goals.[9] In applying this practice, we defined key stakeholders as other federal agencies that work with State on cyber diplomacy efforts. We focused our review on State's activities leading to the development of the June 2019 Congressional Notification on its plan for establishing CSET. We

---

https://www.state.gov/recommendations-to-the-president-on-protecting-american-cyber-interests-through-international-engagement/.

[5]*Cyber Diplomacy Act of 2019*, H.R. 739, 116th Cong. (2019). The House of Representatives passed an earlier version of the bill during the 115th Congress, *Cyber Diplomacy Act of 2017*, H.R. 3776, 115th Cong. (2017).

[6]According to State, the term "cyber diplomacy" encompasses a wide range of U.S. interests in cyberspace. These include cybercrime, cybersecurity, digital economy, international development and capacity building, internet freedom, and internet governance. Others have defined cyber diplomacy as diplomacy in a cyberspace environment, in particular for building strategic international partnerships to support national interests. See A. Barrinha and T. Renard, "Cyber-diplomacy: the making of an international society in the digital age," *Global Affairs*, vol. 3, no. 4-5 (2017); and C. Painter, "Diplomacy in Cyberspace," *The Foreign Service Journal*, vol. 95, no. 5 (2018).

[7]In March 2020, the Cyberspace Solarium Commission recommended, among other things, the creation of a CSET bureau at State, which would report to the Under Secretary of Political Affairs or someone of higher rank. Accessed March 11, 2020. https://www.solarium.gov/report. In July 2020, the National Security Commission on Artificial Intelligence recommended to create a CSET bureau reporting to the Under Secretary for Arms Control and International Security. Accessed September 10, 2020. https://www.nscai.gov/.

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

[9]We did not address agency customers in this review, as they are not relevant to this situation.

also consulted prior GAO work that contained guidance on assessing areas where agencies may be able to achieve greater efficiency or effectiveness by reducing or better managing program fragmentation, overlap, and duplication.[10]

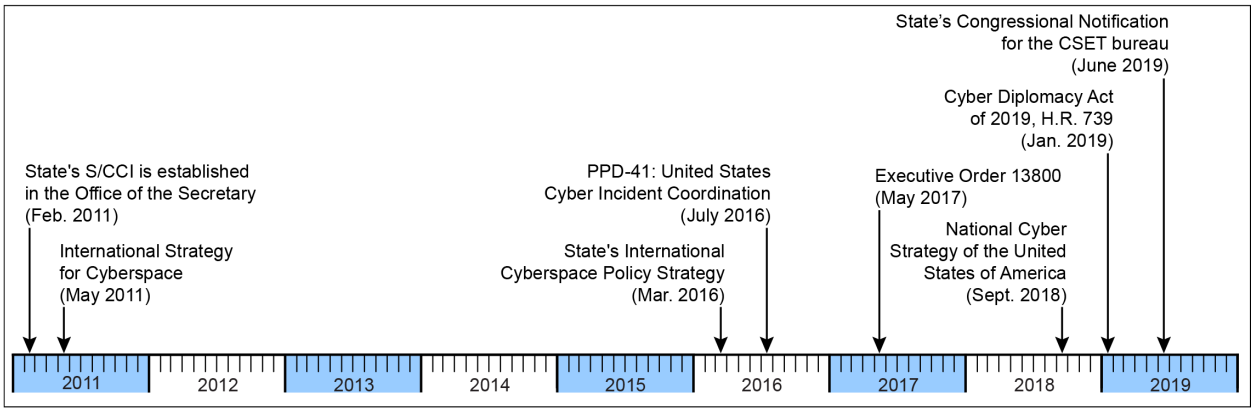
We conducted this performance audit from July 2019 to September 2020 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions 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

State's Role in U.S. Cyber Diplomacy

Since 2011, the United States has recognized the importance of international cyber diplomacy, and State has taken a lead role in carrying out U.S. cyber diplomacy objectives. Figure 1 provides a timeline of key strategies and events in State's involvement in cyber diplomacy.

Figure 1: Timeline of Key Strategies and Events in the Department of State's Involvement in Cyber Diplomacy



Legend: Cyberspace Security and Emerging Technologies = CSET; Department of State = State; Office of the Coordinator for Cyber Issues = S/CCI; Presidential Policy Directive = PPD.

Source: GAO analysis of agency documents. | GAO-20-607R

- In February 2011, State established the Office of the Coordinator for Cyber Issues (S/CCI) in the Office of the Secretary to lead the department's global diplomatic engagement on cyber issues and to serve as liaison to other federal agencies that work on cyber issues.[11]
- In May 2011, the White House issued the *International Strategy for Cyberspace*,[12] which called for strengthening partnerships with other countries to build consensus around

[10]GAO, *Fragmentation, Overlap, and Duplication: An Evaluation and Management Guide*, GAO-15-49SP (Washington, D.C.: Apr. 14, 2015).

[11]In December 2010, State's first Quadrennial Diplomacy and Development Review discussed State's plan to establish S/CCI in the Office of the Secretary.

[12]The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, D.C.: May 16, 2011).

principles of responsible behavior in cyberspace. This strategy included the goal to work with the international community to promote an open, interoperable, secure, and reliable information and communications infrastructure.[13]

- In March 2016, State issued the *International Cyberspace Policy Strategy* report to Congress, as mandated by the Cybersecurity Act of 2015[14], which affirmed the elevation of cyberspace policy as a foreign policy imperative and the prioritization of its efforts to mainstream cyberspace policy issues within the department's diplomatic activities.

- In July 2016, Presidential Policy Directive 41[15] tasked the Cyber Response Group to support the National Security Council (NSC) as the national policy coordination mechanism for significant cyber incidents[16] affecting the U.S. or its interests abroad. In addition to State, other agencies represented in NSC's Cyber Response Group include Commerce, DOD, DOE, DHS, DOJ, and Treasury.

- In May 2017, the White House issued Executive Order 13800, which required, among other things, that the Secretary of State coordinate with other agencies to submit reports to the President on (1) options for deterring adversaries and protecting the United States from cyber threats, and (2) an engagement strategy for international cooperation on cybersecurity.[17]

- In September 2018, the White House issued the *National Cyber Strategy of the United States of America,*[18] which renewed the commitment to expand American influence abroad to protect and promote an open, interoperable, reliable, and secure internet, as one of its 10 objectives.

---

[13]The strategy defined four key characteristics of cyberspace: (1) open to digital innovation; (2) interoperable around the world; (3) secure enough to maintain users' trust; and (4) reliable enough to support their work.

[14]Pub. L. No. 114-113, Div. N.

[15]The White House, *Presidential Policy Directive 41: United States Cyber Incident Coordination* (Washington, D.C.: July 26, 2016).

[16]According to this directive, a cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that a threat source could exploit. Further, a cyber incident (or a group of related cyber incidents) is considered significant when it is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

[17]State released summaries of these two reports in May 2018. According to State officials, State developed these reports in coordination with other executive branch agencies. The first report recommended an approach for imposing consequences on foreign governments responsible for significant malicious cyber activities aimed at harming U.S. national interests. The second report established a set of objectives and associated actions for cyberspace policy to achieve an open, interoperable, reliable, and secure internet.

[18]The White House, *National Cyber Strategy of the United States of America* (Washington, D.C.: Sept. 20, 2018).

State Intends to Establish a Bureau Focused on Cyberspace Security and the Security-Related Aspects of Emerging Technologies

In June 2019, State notified Congress of its intent to establish the new cyberspace and emerging technologies bureau that would report to the Under Secretary for Arms Control and International Security. Under State's plan, a Coordinator and Ambassador-at-Large would lead the new bureau, which would merge staff from S/CCI and the Office of Emerging Security Challenges within the Bureau of Arms Control, Verification, and Compliance.[19] Under this proposal, the new bureau would have a staffing level of 80 full-time employees and a projected budget of $20.8 million.[20]

According to State's Congressional Notification, the department's rationale for creating the new bureau was to (1) align cyberspace security and emerging technologies security issues with its international security efforts, (2) improve coordination with other agencies working on national security issues, and (3) promote long-term technical capacity within the department.

Under State's proposal, CSET would not focus on the economic and human rights aspects of cyber diplomacy issues. According to State officials, while the department recognized the challenges posed by cyberspace, it considered efforts related to digital economy and internet freedom to be separate and distinct from CSET's cyberspace security focus. In contrast, under H.R. 739, State would consolidate cyber diplomacy activities, such as those related to international cybersecurity, digital economy, and internet freedom, in a new office. Under State's plan, the following bureaus would continue to have responsibility for economic and human rights issues in cyberspace:

- The Bureau of Economic and Business Affairs would continue to have responsibility for promoting international engagement on internet governance, digital trade, data privacy, and related issues.

- The Bureau of Democracy, Human Rights, and Labor would continue to lead State's work for promoting internet freedom, such as by working with other nations to protect human rights online.

Other Federal Agencies Contribute to Cyber Diplomacy Efforts and Coordinate with State

Other federal agencies also contribute to cyber diplomacy on a range of issues, such as combatting international cybercrime, deterring malicious cyber activities, and enforcing export controls for technologies that have national security interests. These six agencies—Commerce, DOD, DOE, DHS, DOJ, and Treasury—work on cyber issues with international partners through a number of agency components, bureaus, or offices. For example:

- According to DHS officials, several DHS entities—including the Cybersecurity and Infrastructure Security Agency (CISA), U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and the Transportation Security Administration

[19]Under H.R. 739, the new office of International Cyberspace Policy would report to the Under Secretary for Political Affairs or to an official holding a higher position than the Under Secretary for Political Affairs.

[20]For fiscal year 2021, State's proposed budget request to establish the new bureau is $17.8 million.

(TSA)—work with international partners on a range of cyber issues, such as cybersecurity, countering cybercrime, and critical infrastructure protection. TSA and CISA, for example, conducted a joint exercise with Israeli counterparts geared toward preventing cyberattacks on aviation infrastructure.

- DOJ entities that work with international partners to address cyber threats include the Criminal Division, National Security Division, and the Federal Bureau of Investigation's (FBI) Cyber Division, according to DOJ officials. For example, FBI's Cyber Division has focused on investigating criminal and state-sponsored malicious cyber activity, which has included issues involving technology-related supply chains and cyber risks of emerging technologies, such as 5G, a suite of fifth-generation wireless technologies. In addition, DOJ's Criminal Division has provided investigative, development, and legal assistance to foreign governments relating to cybercrime.

- Treasury's key offices focusing on cyber issues, such as cybersecurity, digital economy, and internet freedom, include the Office of Cybersecurity and Critical Infrastructure Protection and the Office of Intelligence Analysis, according to Treasury officials. Both offices work with the Treasury's Office of International Affairs to coordinate cyber issues related to international finance and technical assistance with external or internal partners.

These six agencies generally work with State on cyber diplomacy issues in a decentralized manner through a number of State bureaus, offices, and overseas missions. Officials from these agencies told us that they work with State both through formal mechanisms, such as NSC's Cyber Response Group, and through informal or ad hoc mechanisms. For example:

- Commerce's components have coordinated with State on a variety of cyber diplomacy issues, according to Commerce officials. For example, the National Institute of Standards and Technology (NIST) has worked with S/CCI and State's Bureau of Economic and Business Affairs on discussions with international organizations and foreign governments to promote the adoption of its risk-based cybersecurity and emerging technologies guidance. The National Telecommunications and Information Administration also has participated in bilateral and multilateral efforts with S/CCI, including engaging with the multistakeholder Internet Governance Forum and the International Telecommunication Union on international cyberspace activities. In addition, the United States Patent and Trademark Office works with the Office of International Intellectual Property Enforcement within the Bureau of Economic and Business Affairs to protect American intellectual property rights and interests abroad.

- Two DOD entities—the Office of the Secretary of Defense for Policy (OSD-P) and the Joint Chiefs of Staff—interact regularly with State on cyber policy issues through NSC's Cyber Response Group, according to DOD officials. In response to international cyber events, OSD-P also coordinates efforts, as needed, with State's S/CCI. Additionally, DOD has contributed to State's cyber efforts, such as State's effort to organize a panel of cyber experts for a forum at the United Nations.

- DOE's Office of International Affairs (IA) works with several State bureaus and offices on cyber diplomacy, according to DOE officials. In particular, depending on the energy-related issue, IA has worked with State regional or functional bureaus as well as S/CCI. IA has also worked with the Bureau of Counterterrorism on issues related to critical energy infrastructure protection.

State Has Not Involved Federal Agency Partners in the Development of Its Plan to Establish a New Cyber Diplomacy Bureau

Officials from six agencies that work with State on cyber diplomacy issues told us that State did not involve them in the development of its plan for CSET and that they were unaware of the plan. State officials confirmed that, as of March 2020, they had not consulted with other agencies about their plan for establishing CSET as described in the department's June 2019 Congressional Notification. Officials from these agencies told us that being informed of State's plan for the new bureau could be helpful for maintaining and improving their ongoing communications and coordination with State. For example:

- DOE officials stated that coordination of international cyber efforts is a challenge for any one agency and highlighted the importance of close interagency coordination of roles and responsibilities in cyberspace.
- DHS officials told us that they would like to be aware of State's activities and would offer insights if they had access to State's CSET bureau plans.
- DOJ officials stated that strategic coordination with other agencies, including State's CSET bureau, is critical for obtaining relevant or usable information for emerging cyber issues.

State has not initiated a process to involve other federal agencies in the development of its plans for the new CSET bureau. As a result, State has not addressed key practices for involving stakeholders in the development of reforms. State officials told us that they were not obligated to consult with other agencies before completing the CSET plan because it was an internal decision. These officials added that they were not consulted by these agencies when they established offices or bureaus responsible for cyber issues. While State is not legally obligated to involve other agencies in the development of its plans for the new bureau, our prior work on government reforms and reorganizations has shown that it is important for agencies to directly and continuously involve key stakeholders, including agencies supporting similar goals, to develop proposed reforms, such as State's plan for establishing CSET.[21]

Without addressing the key reform practice of involving other agencies in its plans for a new cyber diplomacy bureau, State lacks assurance that it will effectively achieve its goals for establishing CSET. Furthermore, because multiple agencies contribute to cyber diplomacy efforts and are engaged in similar activities, State increases the potential for negative effects from fragmentation, overlap, and duplication of efforts if it does not involve agency partners in the development of its plans to reorganize its cyber diplomacy efforts. Potential negative effects include increased costs or inefficiencies from unnecessary overlap or duplication of efforts.

Conclusions

The United States faces expanding cyber threats and the challenge of building international consensus on standards for acceptable state behavior in cyberspace. State leads U.S. government efforts to advance U.S. interests in cyberspace and works with federal agency partners as part of these cyber diplomacy efforts. While State continues to work with other agencies on international cyber issues through formal and informal mechanisms, it has not

[21]GAO-18-427.

informed or involved these agency partners in the development of its reorganization plan for establishing a new bureau focused on cyberspace security and emerging technologies. Without involving other agencies on its reorganization plan, State lacks assurance that it will effectively achieve its goals for establishing this bureau, and it increases the risk of negative effects from unnecessary fragmentation, overlap, and duplication of cyber diplomacy efforts.

Recommendation for Executive Action

The Secretary of State should ensure that State involves federal agencies that contribute to cyber diplomacy to obtain their views and identify any risks, such as unnecessary fragmentation, overlap, and duplication of these efforts, as it implements its plan to establish the Bureau of Cyberspace Security and Emerging Technologies.

Agency Comments and our Evaluation

We provided a draft of this report to State, Commerce, DOD, DOE, DHS, DOJ, and Treasury for review and comment. We received written comments from State, reprinted in the enclosure. State and DHS also provided technical comments, which we incorporated as appropriate. Commerce, DOD, DOE, DOJ, and Treasury informed us that they had no comments.

State did not concur with our recommendation, noting it was unaware that any of the other Executive Branch agencies we spoke with had consulted with State before reorganizing their cyberspace security organizations, and thus suggesting this is not a widely adopted practice in the U.S. government. State also disagreed that it should consider other agencies as stakeholders in an internal State reform and noted the department had consulted with Congress and stakeholders within the department. In addition, State noted that consolidating security-related aspects of cyberspace policy within CSET would enable it to have a more effective engagement with interagency stakeholders by reducing or better managing program fragmentation, overlap, and duplication. Finally, State asserted that its current processes for coordinating with the cited agencies avoid unnecessary fragmentation, overlap, and duplication of cyber diplomacy efforts and it has not proposed changing these processes.

We stand by our recommendation that State should involve other federal agencies it engages with on cyber diplomacy efforts to obtain their views on its plan to establish CSET. Our prior work has shown that successful reforms require an integrated approach that involves key stakeholders and others. As a result, it is important for agencies to directly and continuously involve key stakeholders, such as federal partners, in the development of major reforms. Our review focused on State's planning process for establishing CSET. Other agencies' efforts to create or reorganize their cyberspace security capabilities and organizations were outside the scope of our review. However, as discussed, State leads U.S. government international efforts to advance U.S. interests in cyberspace and coordinates with federal agency partners as part of these efforts. As the lead U.S. agency in carrying out U.S. cyber diplomacy objectives, it is important for State to incorporate leading practices to ensure the successful implementation of its reorganization effort.

We also maintain that State's federal agency partners on cyber diplomacy efforts are key stakeholders, as they work closely with State and contribute to a range of cyber diplomacy efforts. Consulting with these stakeholders on its reorganization plan would enable State to incorporate their insights from a frontline perspective as well as help to facilitate the development of State's reform goals and objectives for CSET. As State noted, other agencies have preceded it in reorganizing or establishing new international cyberspace organizations, and State could benefit from incorporating lessons learned from these prior efforts.

State's rationale for establishing CSET included the need to improve coordination with other agencies working on national security issues, and State commented that the reorganization would enable it to engage more effectively with interagency stakeholders. State also asserted, however, that its current coordination processes avoid fragmentation, overlap, and duplication, and is not proposing to change these processes. It was beyond the scope of our review to evaluate the extent to which State's current cyber diplomacy efforts include fragmentation, overlap, and duplication. However, with multiple agencies involved in cyber diplomacy efforts and supporting similar goals, the potential for negative effects from fragmentation, overlap, and duplication in these efforts exists. State has provided no evidence to support its assertion that its current processes avoid fragmentation, overlap, and duplication, or that its reorganization plan will mitigate any risks. We are continuing to monitor and review State's overall planning process for establishing CSET as part of our ongoing work on this topic.

We are sending copies of this report to the appropriate congressional committees and the Secretary of State, the Secretary of Commerce, the Secretary of Defense, the Secretary of Energy, the Secretary of Homeland Security, the Attorney General, and the Secretary of the Treasury, and other interested parties. 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 us at (202) 512-5130 or MazanecB@gao.gov, or Nick Marinos on (202) 512-9342 or MarinosN@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report were Rob Ball (Assistant Director), Jeremy Latimer (Analyst-in-Charge), Umesh Thakkar, Neil Doherty, and Aldo Salerno. Other significant contributors include Tom Costa, Mark Dowling, Hoyt Lacy, Kush Malhotra, Mary Moutsos, and Sarah Veale.

Brian M. Mazanec
Director, International Affairs and Trade

Nick Marinos
Director, Information Technology and Cybersecurity

Enclosure

Enclosure: Comments from the Department of State

United States Department of State
Comptroller
Washington, DC 20520

SEP - 4 2020

Thomas Melito
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Mr. Melito:

We appreciate the opportunity to review your draft report, "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 Job Code 103681.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

Sincerely,

Jeffrey C. Mounts

Enclosure:
As stated

cc: GAO – Brian Mazanec
T – Christopher A. Ford
OIG - Norman Brown

Department of State Comments on GAO Draft Correspondence

CYBER DIPLOMACY: State Has Not Involved Relevant Federal Agencies in the Development of Its Plan to Establish the Cyberspace Security and Emerging Technologies (GAO-20-607RSU, GAO Code 103681)

The Department of State appreciates the opportunity to comment on GAO's draft report *"Cyber Diplomacy: State Has Not Involved Relevant Federal Agencies in the Development of Its Plan to Establish the Cyberspace Security and Emerging Technologies Bureau"*.

(U) The draft report examines the extent to which State involved other federal agencies in the development of its plan for establishing CSET. To address this objective, the draft report lists several actions the GAO undertook, including "assessing State's efforts against relevant key practices[1] for agency reforms compiled in our June 2018 report on government reorganization." The draft report focused specifically on the "key practice of how, and to what extent the agency has involved other stakeholders in the development of the proposed reforms to ensure the reflection of their views." In addition, the GAO consulted prior GAO work containing "guidance on assessing areas where agencies may be able to achieve greater efficiency or effectiveness by reducing or better managing program fragmentation, overlap and duplication."

(U) The draft report notes that the Department "has not informed or involved… agency partners in the development of its reorganization plan for establishing a new bureau." The agency partners referred to in the draft report are the Departments of Defense, Commerce, Energy, Homeland Security, Justice and Treasury, which also work on cyber security issues. To this point, and recognizing that this GAO review focuses only on the Department of State's efforts to create CSET, the Department is not aware that any of these Executive Branch organization consulted with the Department of State before creating or re-organizing their cyberspace security capabilities and organizations. This would suggest that consulting with outside agencies, prior to creating new organizational entities or reorganizing existing ones, is not a practice widely adopted within the U.S. government, at least in the arena of cyber security. In addition, although the GAO guidance references a key practice of consulting "other stakeholders in the development of the proposed reforms," we note that none of the agencies listed are in fact "stakeholders" in an internal Department of State reform. As actually required, the Department has held extensive consultations with Congressional oversight committee Members and staff. (As befits an entirely internal reform, moreover, the Department also consulted with stakeholders *within* the Department in order to achieve greater efficiency or effectiveness by reducing or better managing program fragmentation, overlap, and duplication in State Department activities.)

(U) The Department has undertaken the creation of the CSET to consolidate within the Department all the relevant parties involved in the national security-related aspects of

[1] The Department notes that the 2018 GAO report referred to contains a list of key questions, vice practices, which USG agencies are not obligated to ask when undertaking organizational reforms. We believe this proposed bureau structure is entirely consistent with Office of Management and Budget (OMB) guidelines, since OMB did not object to, or suggest changes to, the proposed new bureau when briefed about it.

international cyberspace security and the national security-related aspects of emerging technologies policies to ensure well-coordinated international engagements that advance U.S. national security interests. This new Bureau also would facilitate the Department's efforts to better understand the impact of new, emerging and converging technologies on international security and its core foreign affairs function. Additionally, by consolidating security-related aspects of cyberspace policy into one organization within the Department, CSET will in fact enable much more effective State engagement with interagency stakeholders in order to achieve greater efficiency or effectiveness by reducing or better managing program fragmentation, overlap, and duplication in overall U.S. Government activities.

(U) The Department believes the processes currently used to coordinate with the cited agencies on cyberspace security issues avoid unnecessary fragmentation, overlap, and duplication of cyber diplomacy efforts. It is important to recognize that the Department has not proposed changing these processes. Rather, as was briefed to GAO staff, the Office of the Coordinator for Cyber Issues (S/CCI), which is responsible for cyberspace security issues, would move as a unit into the new bureau, with increased resources. To repeat, this is an internal Department of State reform, the goal of which is to enhance the existing State Department role on these issues. The new bureau would continue coordinating with USG agencies, but with the needed support and engagement of additional staff. The Department therefore disagrees with the GAO's conclusion that, because it did not inform or involve certain USG agencies in the development of its internal plan for CSET, it "lacks assurance that it will effectively achieve its goals for establishing this bureau." Accordingly, the Department believes that the report's recommendation that "the Secretary of State should ensure that State involves Federal agencies that contribute to cyber diplomacy to obtain their views and identify any risks, such as unnecessary fragmentation, overlap and duplication of these efforts, as it implements its plan to establish the Bureau of Cyberspace Security and Emerging Technologies" is redundant to what the Department already does.

Text of Enclosure: Comments from the Department of State

Page 1

Thomas Melito Managing Director

International Affairs and Trade

Government Accountability Office

441 G Street, N.W.

Washington, D.C. 20548-0001

Dear Mr. Melito:

We appreciate the opportunity to review your draft report, "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 Job Code 103681.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

Sincerely,

Jeffrey C. Mounts

Enclosure:

As stated

cc: GAO - Brian Mazanec

T - Christopher A. Ford OIG - Norman Brown

Page 2

Department of State Comments on GAO Draft Correspondence

CYBER DIPLOMACY: State Has Not Involved Relevant Federal Agencies in the Development of Its Plan to Establish the Cyberspace Security and Emerging Technologies (GAO-20-607RSU, GAO Code 103681)

The Department of State appreciates the opportunity to comment on GAO's draft report "Cyber Diplomacy: State Has Not Involved Relevant Federal Agencies in the Development of Its Plan to Establish the Cyberspace Security and Emerging Technologies Bureau".

(U) The draft report examines the extent to which State involved other federal agencies in the development of its plan for establishing CSET. To address this objective, the draft report lists several actions the GAO undertook, including "assessing State's efforts against relevant key practices1 for agency reforms compiled in our June 2018 report on government reorganization." The draft report focused specifically on the "key practice of how, and to what extent the agency has involved other stakeholders in the development of the proposed reforms to ensure the

reflection of their views." In addition, the GAO consulted prior GAO work containing "guidance on assessing areas where agencies may be able to achieve greater efficiency or effectiveness by reducing or better managing program fragmentation, overlap and duplication."

(U) The draft report notes that the Department "has not informed or involved… agency partners in the development of its reorganization plan for establishing a new bureau." The agency partners referred to in the draft report are the Departments of Defense, Commerce, Energy, Homeland Security, Justice and Treasury, which also work on cyber security issues. To this point, and recognizing that this GAO review focuses only on the Department of State's efforts to create CSET, the Department is not aware that any of these Executive Branch organization consulted with the Department of State before creating or re-organizing their cyberspace security capabilities and organizations. This would suggest that consulting with outside agencies, prior to creating new organizational entities or reorganizing existing ones, is not a practice widely adopted within the U.S. government, at least in the arena of cyber security. In addition, although the GAO guidance references a key practice of consulting "other stakeholders in the development of the proposed reforms," we note that none of the agencies listed are in fact "stakeholders" in an internal Department of State reform. As actually required, the Department has held extensive consultations with Congressional oversight committee Members and staff. (As befits an entirely internal reform, moreover, the Department also consulted with stakeholders within the Department in order to achieve greater efficiency or effectiveness by reducing or better managing program fragmentation, overlap, and duplication in State Department activities.)

(U) The Department has undertaken the creation of the CSET to consolidate within the Department all the relevant parties involved in the national security-related aspects of

1 The Department notes that the 2018 GAO report referred to contains a list of key questions, vice practices, which USG agencies are not obligated to ask when undertaking organizational reforms. We believe this proposed bureau structure is entirely consistent with Office of Management and Budget (OMB) guidelines, since OMB did not object to, or suggest changes to, the proposed new bureau when briefed about it.

international cyberspace security and the national security-related aspects of emerging technologies policies to ensure well-coordinated international engagements that advance U.S. national security interests. This new Bureau also would facilitate the Department's efforts to better understand the impact of new, emerging and converging technologies on international security and its core foreign affairs function. Additionally, by consolidating security-related aspects of cyberspace policy into one organization within the Department, CSET will in fact enable much more effective State engagement with interagency stakeholders in order to achieve greater efficiency or effectiveness by reducing or better managing program fragmentation, overlap, and duplication in overall U.S. Government activities.

(U) The Department believes the processes currently used to coordinate with the cited agencies on cyberspace security issues avoid unnecessary fragmentation, overlap, and duplication of cyber diplomacy efforts. It is important to recognize that the Department has not proposed changing these processes. Rather, as was briefed to GAO staff, the Office of the Coordinator for Cyber Issues (S/CCI), which is responsible for cyberspace security issues, would move as a unit into the new bureau, with increased resources. To repeat, this is an internal Department of State reform, the goal of which is to enhance the existing State Department role on these issues. The new bureau would continue coordinating with USG agencies, but with the needed

support and engagement of additional staff. The Department therefore disagrees with the GAO's conclusion that, because it did not inform or involve certain USG agencies in the development of its internal plan for CSET, it "lacks assurance that it will effectively achieve its goals for establishing this bureau." Accordingly, the Department believes that the report's recommendation that "the Secretary of State should ensure that State involves Federal agencies that contribute to cyber diplomacy to obtain their views and identify any risks, such as unnecessary fragmentation, overlap and duplication of these efforts, as it implements its plan to establish the Bureau of Cyberspace Security and Emerging Technologies" is redundant to what the Department already does.

(103681)