Congressional Notification for
Proposed Bureau of Cyberspace Security and Emerging Technologies

BACKGROUND

The Department intends to establish a new Bureau of Cyberspace Security and Emerging Technologies (CSET). In considering the growing national security challenges presented by cyber space and emerging technologies, the Department has determined that its efforts in these areas are not appropriately aligned or resourced. After much consideration, the Department has determined that the best way to more effectively address the security, economic, and human rights aspects of these issues is to do the following: (1) create a new bureau to consolidate resources focused on cyberspace security and the security-related aspects of emerging technologies, (2) increase the existing Bureau of Economic and Business Affairs' focus on the digital economy and privacy aspects of cyberspace and emerging technologies; (3) retain in the Democracy, Human Rights, and Labor Bureau its important work on Internet Freedom[1].

CSET would report to the Under Secretary for Arms Control and International Security, and would be led by a Coordinator and Ambassador-at-Large for Cyberspace Security and Emerging Technologies who would have a status equivalent to an Assistant Secretary and would be subject to Senate advice and consent.[2] The new bureau would unify the policy functions and align national security responsibilities related to cybersecurity and emerging technologies with the Department's international security efforts, facilitate coordination with fellow national security agencies, and promote the Department's long-term technical capacity in these areas.

The Bureau of Economic and Business Affairs ("EB") would continue to promote U.S. economic competitiveness through international engagement on Internet governance, digital trade, innovative technologies, data privacy, and information and communications policy. EB would continue to interact with the private sector, international organizations, civil society, and foreign governments and regulators to advance U.S. digital economy interests.

To ensure that the Department's work on the economic, commercial and privacy aspects of cyberspace and emerging technologies continues to be appropriately prioritized, EB plans to increase focus on: (1) developing and implementing diplomatic strategies to

---

[1] Reflecting long-standing practice at the State Department, the Bureau of Democracy, Human Rights, and Labor will remain chiefly responsible for promoting Internet freedom and administering related programs.

[2] Under section 1(c)(1) of the State Department Basic Authorities Act of 1956, the Department is limited to a total of 24 Assistant Secretary of State positions. To accommodate this limitation, the Department proposes to have an Ambassador-at-Large with Assistant Secretary equivalency lead the new bureau.

ensure that the Internet remains open and interoperable and protects the free flow of information; (2) encouraging international adoption of a pro-growth, pro-innovation digital regulatory landscape that is technology-neutral; (3) advocating on behalf of U.S. companies and coordinating domestic and international engagements to advance U.S. business interests in innovative technology sectors; (4) promoting U.S. exports of information and communications technology equipment and services; and (5) leading State Department engagement on data privacy and EU-U.S. and Swiss-U.S. Privacy Shield.

As part of this effort, the Department plans to restore the rank of Ambassador-at-Large to the EB official overseeing these issues. The Department will shortly provide to Congress a proposal, including additional resources, as required, outlining the specific details of EB's planned reorganization.

KEY STAFFING AND FINANCIAL PLAN

The new CSET bureau would have a proposed staffing level of 80 FTE and a projected budget of $20.8 million. As set forth in the table below, CSET would attain these staffing and budget levels in two phases.

- In Phase 1, the Office of the Coordinator for Cybersecurity (S/CCI), which has 22 FTEs, would be realigned to the CSET bureau. In addition, nine (9) FTEs from the Bureau of Arms Control, Verification and Compliance, Office of Emerging Security Challenges (AVC/ESC), to include associated salaries and bureau-managed operational and program funds and current areas of responsibility, would be realigned to the CSET bureau. In Phase 1, the overall budget impact is resource neutral. At the conclusion of Phase 1, CSET would include a total of 31 existing FTEs and a budget of $7 million, of which $3.9 million would be American salaries and $3.1 million would be bureau-managed funds.

- In Phase 2, 26 FTE positions would be realigned in FY 2019 from the HR Special Complement, with an additional 23 FTE to be realigned in FY 2020. The projected budget for Phase 2 would be $13.8 million, of which $7.1 million would be American salaries for 49 FTEs and $6.7 million would be bureau-managed funds.

The following table displays Phase 1 and Phase 2 FTE and budget estimates:

Planned Bureau of Cyberspace Security and Emerging Technologies (CSET)
($ in Thousands)

Diplomatic Programs Account (D&CP)	Direct Funded American Positions	Centrally-Managed Salaries	Bureau-managed funds
Phase 1			
Reprogramming From:			
Office of the Coordinator for Cyber Security (S/CCI) (Office of the Secretary)	22 positions	$2,885	$2,612
Arms Control, Verification and Compliance, Office of Emerging Security Challenges and Defense Policy (AVC/ESC)	9 positions	$1,018	$526
Total Reprogramming From:	**31**	**$3,903**	**$3,138**
Reprogramming To:			
Cyberspace Security and Emerging Technologies (CSET) Bureau	**31**	$3,903	$3,138
Phase 2			
Realigned from HR Special Complement: FY2019	26	$3,761	$1,942
Realigned from HR Special Complement: FY 2020	23	$3,326	$1,717
Other budget items			$3,035
Total Phase 2:	**49**	**$7,087**	**$6,694**
Total of Phases 1 and 2	**80**	**$10,990**	**$9,832**

DESCRIPTION OF THE REORGANIZATION

CSET would lead U.S. government diplomatic efforts to secure cyberspace and its technologies, reduce the likelihood of cyber conflict and prevail in strategic cyber competition. CSET would be led by an Ambassador-at-Large with status equivalent to an Assistant Secretary and one Principal Deputy Coordinator who supervises two Deputy Coordinators. The three Deputy Coordinators would have status equivalent to Deputy Assistant Secretaries. The Principal Deputy Coordinator would oversee one office, while the other two Deputy Coordinators would each oversee one of CSET's two directorates as the Deputy Coordinator for International Cyberspace Security and the Deputy Coordinator for Emerging Technologies and Information Infrastructure Security.

Attached are the current organizational charts and the proposed charts with the number of FTEs shown in each office.

The organizational responsibilities of CSET would be as follows:

Coordinator and Ambassador-at-Large
The Coordinator and Ambassador-at-Large would lead U.S. diplomatic efforts on a wide range of international cybersecurity and emerging technologies policy issues that impact U.S. foreign policy and national security in order to secure cyberspace and related technologies, reduce the likelihood of cyber conflict and prevail in strategic cyber competition. The Ambassador-at-Large would also be responsible for overseeing policy and resources within the Department on matters relating to cyberspace security, security-related aspects of emerging technologies, and certain outer space matters.

Principal Deputy Coordinator
The Principal Deputy Coordinator would oversee the Office of Planning, Cybersecurity Assistance and Communications, which would be responsible for the Bureau's strategic planning, including the management of Diplomatic Programs (DP) and foreign assistance funding. The Office of Planning, Cybersecurity Assistance and Communications also would direct public diplomacy, media, and legislative affairs activities for the Bureau to ensure consistency with Administration messaging, and plan and execute relevant Department-wide policy training.

Deputy Coordinator for International Cyberspace Security
The Deputy Coordinator for International Cyberspace Security would lead the Department's global diplomacy engagement on cyberspace security issues; build the capacity of U.S. diplomatic officials to engage on global cybersecurity issues; and on the U.S. approach to deter and counter malicious cyber actors; promote agile collaboration with allies and partners to identify, counter, and deter destabilizing state behavior in cyberspace; and implement programs to build foreign partner capacity to increase resilience, address cyberspace threats, and construct and reinforce voluntary, non-binding norms of responsible state behavior in cyberspace.

Office of Global Policy, Plans and Negotiations (CSET/GPPN)
CSET/GPPN would develop, advance, and negotiate the implementation of key international cyberspace security policies directed by national-level guidance; manage international and interagency policy coordination; serve as the State Department's primary representative to coordination meetings convened by the National Security Council (NSC) for cyberspace security policy issues; and support the Under Secretary for Arms Control and International Security and other senior Department officials for NSC and other interagency meetings, as required.

Office of International Engagement and Capacity Building (CSET/IECB)
CSET/IECB would cultivate and manage relationships with key bilateral, multilateral and international entities (regional and international organizations) in support of national cyberspace security-related foreign policy objectives; and develop and implement capacity-building programs to support cyberspace security policy objectives, such as the development of national cyberspace security plans and confidence-building measures to strengthen the capabilities necessary to prevent, detect, and respond to cyberspace threats.

Office of Threat Management and Operational Coordination (CSET/TMOC)
CSET/TMOC would provide adversary-specific policy expertise to counter and contest malicious cyberspace actors, including influence operations and other malign cyberspace-enabled techniques; coordinate internationally with other governments and facilitate U.S. cyberspace operations; and advise Department leadership on cyberspace operations issues, incidents, and campaigns.

Deputy Coordinator for Emerging Technologies and Information Infrastructure Security
The Deputy Coordinator for Emerging Technologies and Information Infrastructure Security would be responsible for management of the international security issues posed by emerging and converging technologies and critical information infrastructure, eg. new threats in outer space, Artificial intelligence (AI), quantum computing, and biotechnology, among others, as they are identified . Such technologies commonly possess a wide range of potential applications and can have dual-use concerns related to international security. Based on the U.S. government's national security goals related to emerging technologies and information infrastructure, the Deputy Coordinator would develop and implement the Department's policy positions and diplomatic engagements; lead the Department's efforts to develop non-binding norms of responsible state behavior in the development and use of emerging/converging technologies; address issues related to state and non-state actor acquisition and misuse of emerging/converging technologies; lead in the engagement with international organizations focused on the security aspects of emerging/converging security technologies; and coordinate across the Department to ensure a consistent approach to issues related to dual-use or civil/commercial uses of emerging technologies.

Office of Emerging Technology Security and Outreach (CSET/ETSO)
CSET/ETSO would manage policy development and enhance understanding regarding national security implications of emerging technologies; develop, in coordination with relevant partners from within the U.S. government, and as needed, from industry, academia and non-governmental organizations, proposals for non-binding norms of responsible state behavior related to emerging technology security issues; and conduct international outreach to ensure coordination among key allies and partners to oppose efforts to establish international frameworks that would be detrimental to U.S. national security interests related to these technologies.

Office of Critical Information Infrastructure Security (CSET/CIIS)
CSET/CIIS would develop and implement policies, and conduct outreach designed to enhance and protect the security of international critical information infrastructure, and maintain the resilience of communications, to include infrastructure in a variety of domains and political jurisdictions, such as outer space and undersea.

RATIONALE AND ADDITIONAL INFORMATION

With the proposed new bureau, all the relevant parties involved in cyberspace security and the security-related aspects of emerging technologies policies would be housed in the same bureau to ensure well-coordinated international engagements in bilateral and multilateral venues to advance U.S. national security interests. These critical diplomatic and programmatic initiatives/efforts can best be achieved by a fully staffed and focused CSET Bureau, led by an Ambassador-at-Large with status equivalent to an Assistant Secretary, who reports to the Under Secretary of Arms Control and International Security (T). Because of the complex nature and dual-use of many of the technologies that would fall under the responsibility of the CSET Bureau, T would continue to coordinate with other bureaus to address any cross-cutting issues. The proposed structure would also allow the Department to address more effectively cross-cutting issues such as cyberspace and outer space security issues. Further, this new structure would facilitate the Department's efforts to better understand the security impact of new, emerging and converging technologies on international security.

By creating the new CSET bureau reporting to T, the Department would align cyberspace security and emerging technologies security issues with the Department's international security efforts, improve coordination with fellow national security agencies, and promote long-term technical capacity at the Department. With existing and new assets and the right structure, the Department would have the capacity to respond in a coordinated and timely manner to 21st century cyberspace security threats and address in a coordinated and comprehensive manner the national security challenges presented by newly emerging technologies. The proposed changes would bolster the U.S. Government's capabilities to engage more broadly and deeply on our global cyberspace security priorities.

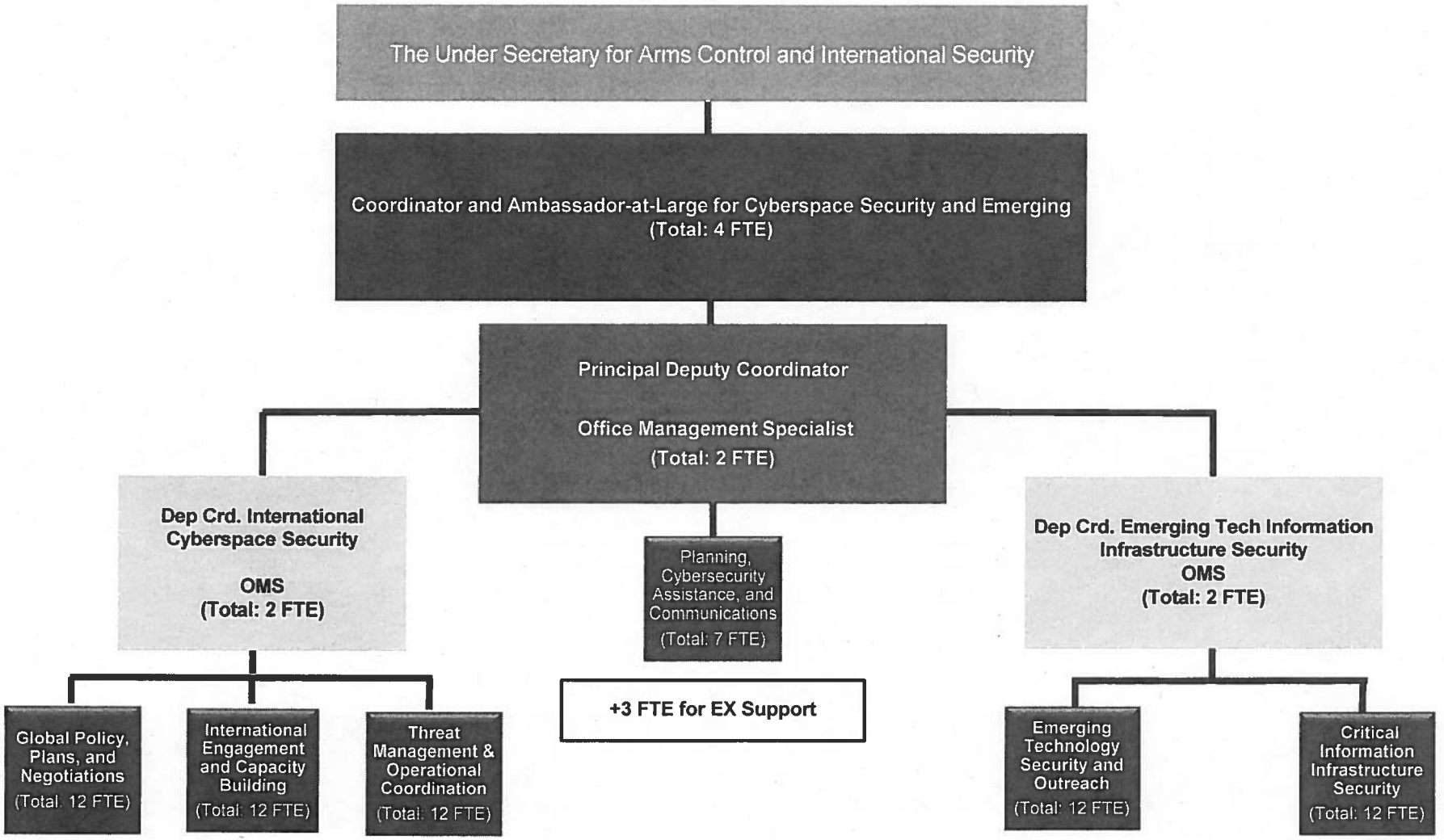
The Department would begin implementation once congressional and union notification procedures have been completed. Implementation of Phase 1 is expected to take three months. Phase 2 would be implemented in FY 2019 (realignment of 23 FTEs) and in FY 2020 (realignment of 26 FTEs). Resources for contracts and travel are included in the estimated costs for the new bureau and are reflected in the figures in the table above. All space, including secure space, requirements with their associated costs will be determined and provided separately.

The creation of CSET would allow for better prioritization of foreign assistance programs for cyberspace security projects and projects involving the national security aspects of emerging technologies, and ensure there is appropriate policy coordination and oversight across these foreign assistance objectives. Funding for programs that support Internet freedom would remain under the Bureau of Democracy, Human Rights and Labor.

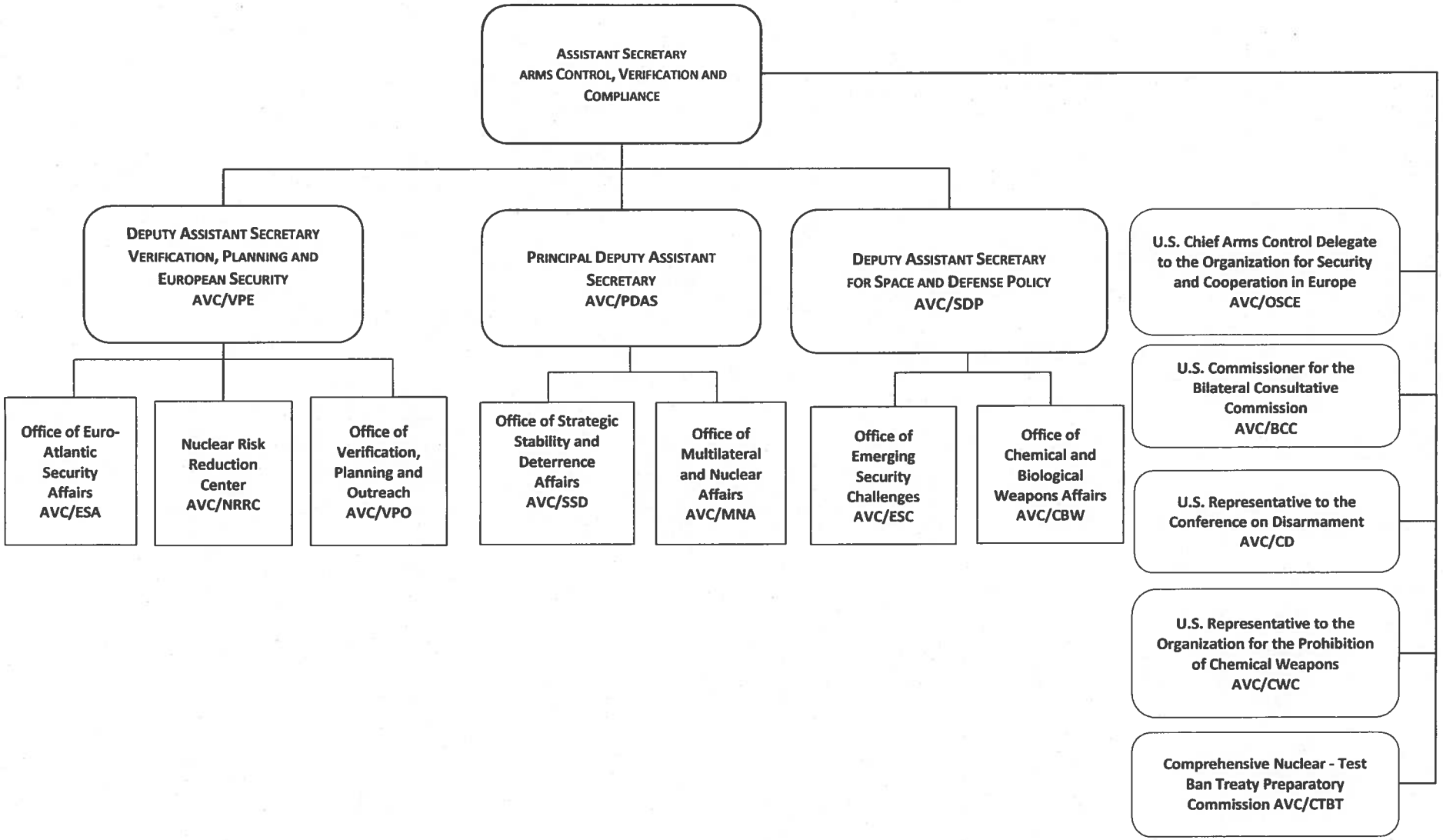
Committee Use Only || Not for Public Release

DRAFT/PRE-DECISIONAL

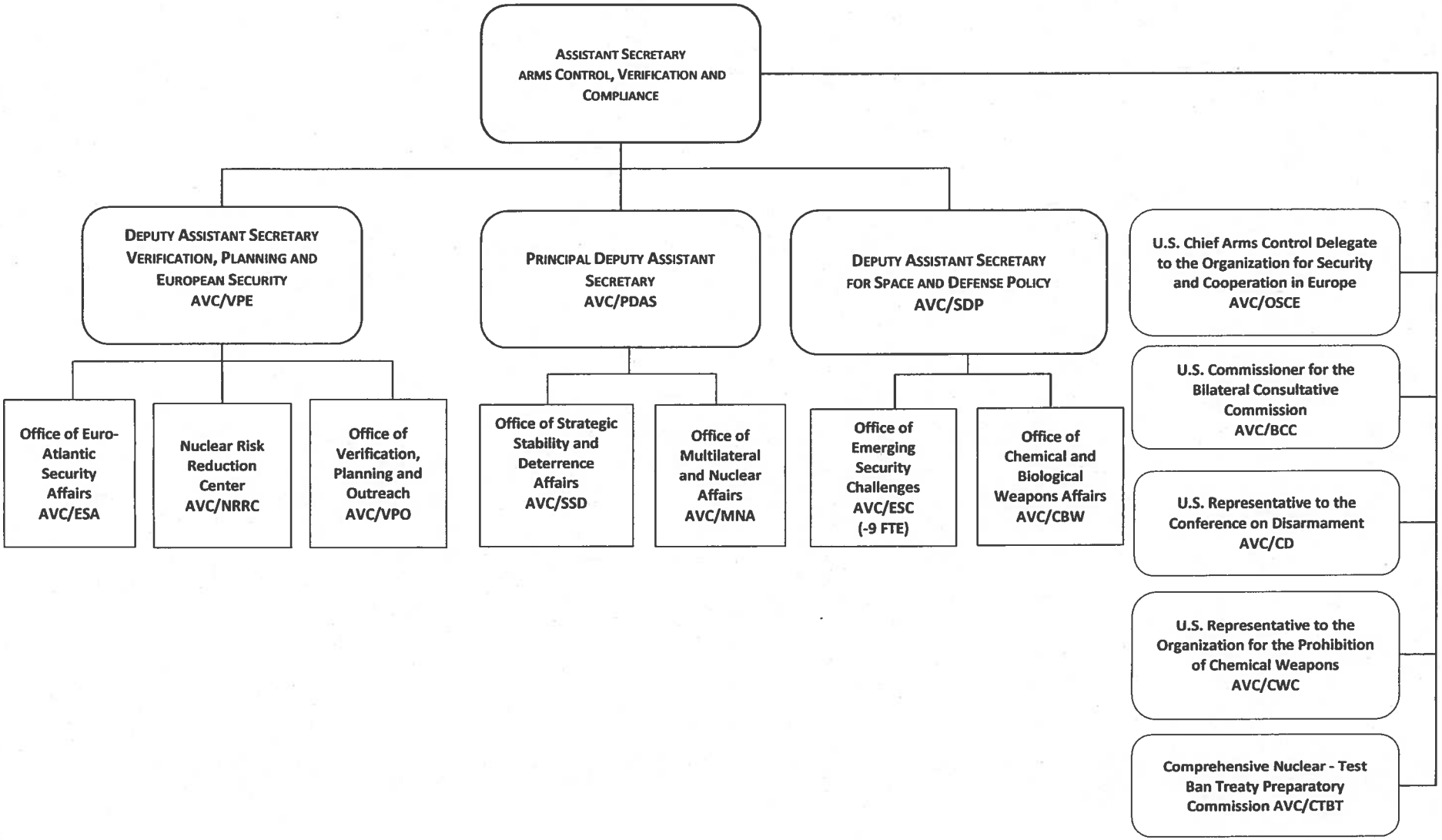
Bureau of Cyberspace Security and Emerging Technologies
80 FTE



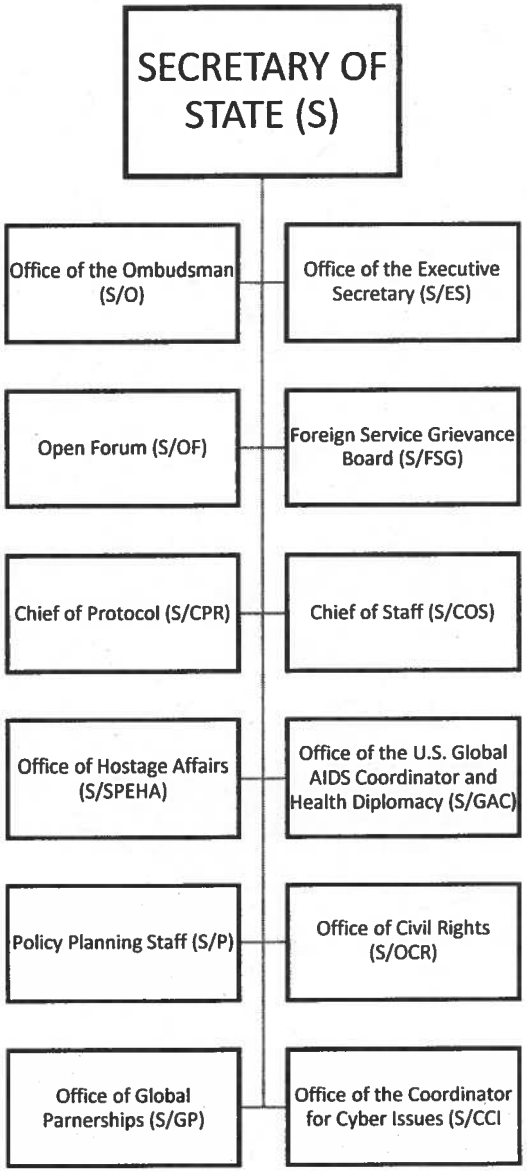
Bureau of Arms Control, Verification and Compliance (AVC) – CURRENT



Bureau of Arms Control, Verification and Compliance (AVC) – PROPOSED



Office of the Secretary of State (S) – CURRENT



Office of the Secretary of State (S) – PROPOSED