Appendix 1: Summary of Recommendations

Objective	Actions	Timeline	Implementing US Gov. Entity
1. Create and empower a National Cyber Advisor (NCA) position within the Executive Office of the President (EOP).[1]	1.1 The NCA should be located within the EOP.	Day 0	White House
	1.2 The NCA should be a National Security Council (NSC) deputy.		
	1.3 The NCA should not require Senate confirmation.		
	1.4 The NCA should be supported by an Office of the National Cyber Advisor (ONCA).		
	1.5 The ONCA should play a role in planning, organizing, and overseeing strategic disruption of criminal infrastructures.		
	1.6 The ONCA should be allotted a staff of 25-30 people.		
	1.7 The ONCA should have dedicated funding within the EOP budget.		
	1.8 The ONCA should concurrently review federal cybersecurity budgets with the Office of Management and Budget (OMB).		
	1.9 The ONCA should be transparent about its interaction with the private sector.		
	1.10 The ONCA should prioritize transparency by publishing an annual report.		
2. Enable the ONCA to coordinate with federal agencies to identify, resolve, and develop proposals to improve interagency processes and federal partnerships with external stakeholders to close the cyber enforcement gap	2.1 The ONCA should lead a temporary, intergovernmental Cybercrime Working Group that consists of the Departments of Justice (DOJ), Homeland Security (DHS), State (DOS), Treasury, and the Federal Bureau of Investigation (FBI), US Secret Service (USSS), and other relevant federal entities to assess and develop interagency policies and legislative proposals on cybercrime and cyber enforcement, particularly in areas where cross-agency coordination and cooperation is required, and to coordinate with the private sector and SLTT partners when necessary.	0-100 Days	ONCA

1 At the time of writing, Congress has pending legislation to create a National Cyber Director (NCD) that would perform similar, but not all, of the duties recommended in this report. The legislation authorizes this position at the Director level but for the purposes of this publication the term "National Cyber Advisor" will be used to refer to this position. See: Section 1132 of the FY 2021 National Defense Authorization Act (H.R. 6395): https://www.congress.gov/116/bills/hr6395/BILLS-116hr6395pcs.pdf.

3. Introduce legislation that permanently places the Vulnerabilities Equities Process (VEP) under the purview of the ONCA and increases the transparency of the VEP.	3.1 The NCA should work with Congress to develop legislation establishing a permanent Equities Review Board (ERB) within the ONCA.	0–100 Days	White House (with Congress)
	3.2 In this legislation, Congress should establish a permanent VEP Director position to lead the ERB, supported by an Executive Secretariat.		
	3.3 Congress should require all US government agencies to timely submit all known vulnerabilities for review by the ERB.		
	3.4 Congress should require the VEP Executive Secretariat to publish an annual report about the ERB.		
	3.5 The VEP Director should clarify that the VEP applies to both purchased and internally discovered vulnerabilities.		
	3.6 The VEP Director should ensure that voting power within the ERB is distributed equitably and should clarify the process to resolve disagreements.		
	3.7 The VEP Director should establish procedures for conducting regular reviews of the ERB.		
4. Update the US government's approach to cyber threat intelligence collection and sharing around cybercrime.	4.1 The Office of the Director of National Intelligence (ODNI) and the ONCA should create a joint working group to identify intelligence collection gaps on cybercrime and propose ways to close those gaps.	0–100 Days	ODNI and ONCA
	4.2 The ONCA should integrate functional intelligence collection priorities related to cybercrime into regional intelligence priorities.	101–180 Days	ONCA
	4.3 The ONCA should work with the Intelligence Community (IC) to update US government cyber threat intelligence analysis to produce adversary playbooks that describe cyber threat actors' typical tactics, techniques, and procedures.	Day 0	ONCA
	4.4 The Cybercrime Working Group should enhance effective intergovernmental and public information sharing about cyber threat vectors, including those related to cybercrime.	0–100 Days	Cybercrime Working Group
	4.5 The Director of National Intelligence (DNI) shall prepare a National Intelligence Estimate (NIE) on the relationship between criminal cyber actors and nation-states.	Day 0	ODNI
5. Develop a dedicated strategic approach to cyber enforcement as part of a US national cyber strategy.	5.1 The NCA should target a specific amount by which to reduce the economic impact of cybercrime by 2024.	101–180 Days	ONCA
	5.2 ONCA staff should consult the private sector and civil society groups to identify barriers to the reduction of the economic impact of cybercrime.	101–180 Days	
	5.3 The NCA should work through an interagency process to immediately draft a cybercrime addendum to the 2018 National Cyber Strategy and eventually strengthen the cybercrime components of a new or updated national cyber strategy.	101–180 Days	

6. Identify and clarify roles and responsibilities among federal and state, local, tribal, and territorial (SLTT) criminal justice agencies to strengthen institutionalized processes and relationships with public, private, and international partners to improve cybercrime investigations and prosecutions.	6.1 The Cybercrime Working Group should clearly delineate cyber enforcement roles and responsibilities within federal entities, and between federal and SLTT, private, and international partners to create more effective, interagency coordination.	101–180 Days	Cybercrime Working Group
7. Increase prioritization of cybercrime among federal, SLTT, and private sector stakeholders and direct federal resources to federal and SLTT agencies that are commensurate with its prevalence and impact.	7.1 OMB and the ONCA should review all federal departments and agencies with cyber enforcement missions to create a comprehensive cyber enforcement budget proposal for the President's Budget Request for FY 2023 or FY 2024.	101–180 Days	OMB and ONCA
	7.2 The ONCA should develop a plan to attend and hold a series of forums and workshops with SLTT and private sector participants to discuss challenges of cyber enforcement and areas to improve partnerships.	0–100 Days	ONCA
8. Develop uniform metrics to inform and improve data reporting, victim response, and national data collection for federal and SLTT law enforcement.	8.1 The ONCA should consult with relevant federal departments and agencies to develop uniform metrics to evaluate the federal government's efforts to reduce cybercrime and to inform data collection efforts.	101–180 Days	ONCA
	8.2 DOJ and FBI should develop policies and legislative proposals to expand cybercrime categories in the National Incident-Based Reporting System (NIBRS), further spur the uptake of NIBRS, and explore other initiatives to improve data reporting.	1 Year+	DOJ and FBI
	8.3 To improve law enforcement's response to victims, the Cybercrime Working Group should develop proposals that improve cybercrime reporting among public and private victims and the assistance awarded to them.	1 Year+	Cybercrime Working Group
9. Strengthen federal and SLTT law enforcement's ability to share investigative information related to cybercrime.	9.1 The Cybercrime Working Group should develop policies and propose additional funding to strengthen existing information sharing mechanisms to enable investigations by criminal justice agencies.	1 Year+	Cybercrime Working Group

10. Improve the digital evidence forensic capacity and capability of federal and SLTT criminal justice agencies by reforming recruitment, training, and retention practices.	10.1 The Office of Personnel Management (OPM) and OMB should issue a memorandum that outlines policy proposals and propose funds for FY 2023 and/or FY 2024 to improve recruitment practices for federal law enforcement agencies regarding cyber enforcement personnel.	101–180 Days	OPM and OMB
	10.2 In their updated memorandum, OPM and OMB should include policy proposals and propose funds for FY 2023 and/or FY 2024 to expand training opportunities for federal and SLTT law enforcement and other criminal justice agencies and retain those employees once trained.	101–180 Days	OPM and OMB
	10.3 The ONCA should work with Congress to develop legislation to ensure that federal and SLTT criminal justice agencies have access to technical assistance to examine digital evidence.	0–100 Days	ONCA
	10.4 DOJ should develop policies and request sufficient funding so that federal and SLTT criminal justice agencies have access to technical assistance to examine digital evidence.	0–100 Days	DOJ
11. Assess the needs, resources, and capacity of SLTT criminal justice agencies and federal–state collaborative organizations to address cybercrime.	11.1 DOJ should coordinate with DHS to assess the gap between the needs of SLTT criminal justice agencies and their capabilities and capacities.	0–100 Days	DOJ and DHS
	11.2 DOJ should determine how many localities are using the Edward Byrne Memorial Justice Assistance Grant (JAG) program for cybercrime initiatives, how much these localities have received for these initiatives, how the program could be used to promote SLTT cyber enforcement, and whether other grant programs should be expanded.	0–100 Days	DOJ
	11.3 DOJ and DHS should identify and recommend proposals on how to improve and expand federal and SLTT cybercrime task forces.	0–100 Days	DOJ and DHS
12. Establish a new structure in the Department of State (DOS) to ensure a well-resourced single point of high-level leadership for all cyber diplomacy matters, backed by an architecture that allows for other bureaus advancing policy and programming on cybercrime to effectively coordinate.	12.1 The Secretary of State should establish an Office of International Cyberspace Policy at DOS with the head of Office having the rank and status of Ambassador and ensure this Office is supported with the adequate funding and personnel to fulfill its mandate.[2]	0–100 Days	DOS
	12.2 The White House should work with Congress to codify the Office of International Cyberspace Policy at DOS.	0–100 Days	White House

2 The Secretary should consider appointing the head of such an Office at the rank of Assistant Secretary or higher in compliance with statutory restrictions.

13. Identify a set of diplomatic tools and policy options to boost international cooperation in cybercrime investigations and address governments that are systematically uncooperative.	13.1 DOS, in coordination with the White House and all relevant departments and agencies in the US government, including the IC, should draft a new US global cyber engagement strategy through an interagency process. This strategy should be updated every four years and inform the development of a national cyber strategy by the White House.	1 Year+	DOS
	13.2 Once a new global cyber engagement strategy is issued, all regional DOS bureaus and USAID should be required to update or draft new regional cyber strategies to align with the newly established goals and objectives.	1 Year+	DOS
	13.3 DOS should include cybercrime and other cyber priorities in other key review and strategic planning documents for the Department and USAID. This should include any and all future Quadrennial Diplomacy and Development Reviews (QDDR).	1 Year+	DOS
	13.4 DOS should enhance its training and awareness raising on cybercrime for policy officers at posts, encourage posts to add cybercrime as a standing item to Law Enforcement Working Groups, identify additional Department-wide training opportunities to enhance training and awareness on cybercrime, and dedicate time at annual Chiefs of Mission meetings for updates on cyber developments.	101–180 Days	DOS
	13.5 The Department of Treasury, in coordination with all relevant departments and agencies including the IC, should undertake an inter-agency assessment of the effectiveness of all existing cyber-related sanctions in halting or reducing malicious cyber activity.	101–180 Days	Treasury Department
	13.6 DOS, in cooperation with the Department of Treasury, should increase support to non-governmental research institutions to conduct regular, independent assessments of the effectiveness of cyber sanctions and propose recommendations to improve the US's cyber sanctions regime.	1 Year+	DOS
	13.7 Should the United States choose to participate in negotiations on a new global cybercrime convention, it should develop a strategy for engagement and ensure the process is transparent, inclusive, and safeguards human rights.	1 Year+	White House

14. Identify a group of countries where the US government is not receiving timely assistance in cybercrime investigations and develop programs to support their criminal justice capacity building needs—including operational support, policy development, and harmonization of laws—to boost cooperation.	14.1 As part of the development of a new global cyber engagement strategy, DOS should work in cooperation with USAID, DOJ, FBI, the IC, and all other relevant federal entities to develop an assessment, monitoring, and evaluation (AM&E) framework for all cyber foreign capacity building programs funded through annual foreign assistance resources. This AM&E framework should inform and ultimately be integrated into a broader DOS security sector assistance AM&E framework.	181 Days–1 Year	DOS
	14.2 The DOS Office of International Cyberspace Policy, in partnership with the International Narcotics and Law Enforcement Bureau (INL) and relevant federal entities, should lead a process that identifies a target number of countries where the US government is not receiving timely assistance in cybercrime investigations and it is determined that increased support to their cyber capacity building needs may have an impact.	1 Year+	
	14.3 DOS should take steps to establish regional and/or in-country donor coordination mechanisms on cyber capacity building to overcome the duplication in funding that has been observed from donor governments.	1 Year+	
15. Streamline the process and improve the timeline for responding to cross-border data requests, in accordance with substantive and procedural protections.	15.1 DOJ, in cooperation with DOS, should strengthen prioritization within the US government for the signing of new executive agreements under the "Clarifying Lawful Overseas Use of Data Act" (CLOUD), institute transparency in the process for the negotiation of CLOUD Act agreements, and ensure CLOUD Act agreements are not used as a means for facilitating a backdoor to decryption mandates or other misuses prohibited by the law.	Continuous	DOJ and DOS
	15.2 DOJ should update guidance on the CLOUD Act, as necessary, to clarify for foreign partners and domestic audiences what the law does and does not do and provide information to those that may misunderstand its intent and scope.	Continuous	DOJ
	15.3 DOJ, in cooperation with DOS, should work to conclude negotiations around the Second Additional Protocol to the Budapest Convention as a means of facilitating more efficient cross-border data sharing while ensuring due process and the protection of civil liberties, and begin work with Congress and the private sector to prepare for implementing legislation.	Continuous	DOJ
	15.4 The Attorney General should direct entities within DOJ to adopt recommendations to make the MLAT system more effective and efficient and ensure the annual budget request reflects the resources needed to implement them.	101–180 Days	DOJ

	15.5 DOJ should establish a system to allow for public reporting of MLAT data, including the number of inbound and outbound MLAT requests processed and the average processing time of inbound and outbound requests.	181 Days–1 Year	DOJ
	15.6 The Attorney General should direct DOJ to provide any necessary additional resources for attaches, legal and cyber advisors, and other personnel placed in foreign missions to meet their mission. DOJ, in cooperation with the FBI and DOS, should evaluate whether decisions are being made as to where to deploy such resources based on a strategic approach and with adequate criteria. DOJ, DOS, and the FBI should work with Congress to authorize and appropriate resources to support increases in personnel as necessary to meet the need.	101–180 days	DOJ
16. Establish processes at lead agencies to measure the implementation of all objectives	16.1 As part of the implementation of each of these recommendations, the lead department or agency for each should establish a process to set a timeline for implementation and a mechanism to monitor implementation and measure impact.	Continuous	All lead departments and agencies