STRATEGIC OBJECTIVE #3:

REFORM THE EXECUTIVE BRANCH TO BE MORE AGILE AND EFFECTIVE IN CYBERSPACE

The executive branch should be restructured and streamlined in order that clear responsibilities and authorities over cyberspace can be established while it is empowered to proactively develop, implement, and execute its strategy for cyberspace. Many departments and agencies, with different responsibilities for and interests in securing cyberspace, compete for resources and power, resulting in conflicting efforts sometimes carried out at cross-purposes. More consolidated accountability for harmonizing the executive branch's policies, budgets, and responsibilities in cyberspace while it implements strategic guidance from the President and Congress is needed to achieve coherence in the planning, resourcing, and employing of government cyber resources.

Key Recommendation

1.3 Congress should establish a National Cyber Director (NCD), within the Executive Office of the President, who is Senate-confirmed and supported by the Office of the National Cyber Director. The NCD would serve as the President's principal advisor for cybersecurity and associated emerging technology issues; the lead for national-level coordination for cyber strategy, policy, and defensive cyber operations; and the chief U.S. representative and spokesperson on cybersecurity issues.

The NCD would be appointed by and report directly to the President, be Senate-confirmed, and be supported by a concurrently established Office of the National Cyber Director inside the Executive Office of the President (EOP). (It thus would be positioned similarly to the Office of the U.S. Trade Representative.) The NCD nomination to the Senate would be considered by both the Armed Services and Homeland Security and Governmental Affairs Committees, until and unless a Select Committee on Cybersecurity (recommendation 1.2) is established, at which time the latter committee should assume primary jurisdiction over the NCD nomination and office.

Numerous commissions, initiatives, and studies have recommended a more robust and institutionalized national-level mechanism for coordinating cybersecurity and associated emerging technology issues, and for overseeing the executive branch's development and implementation of an integrated national cybersecurity strategy. As emerging technology- and cyberspace-related issues become more complex, and consequently a greater threat to U.S. national security, the President's need for sound advice and timely options will be increasingly critical.

The NCD would not direct or manage day-to-day cybersecurity policy or the operations of any one federal agency, but instead will be responsible for the integration of cybersecurity policy and operations across the executive branch. Specifically, the NCD would (1) be the President's principal advisor on cybersecurity and associated emerging technology issues and the lead national-level coordinator for cyber strategy and policy; (2) oversee and coordinate federal government activities to defend against adversary cyber operations inside the United States; (3) with concurrence from the National Security Advisor or the National Economic Advisor, would convene Cabinet-level or National Security

Council (NSC) Principals Committee–level meetings and associated preparatory meetings; and (4) would provide budgetary review of designated agency cybersecurity budgets.

Structure and Responsibilities: The NCD, supported by the Office of the National Cyber Director within the White House's EOP, would report directly to the President. The NCD would serve on the NSC for relevant (cybersecurity and associated emerging technology) issues. The NCD would lead the development and coordination of national-level cyber strategy, cyber policy, and defensive cyber operations, including working through the NSC process to set national-level priorities and produce the National Cyber Strategy of the United States. The NCD would also lead White House efforts to support and develop the private-public collaboration needed to defend our national critical infrastructure and provide coordination on emerging cross-cutting technology and security challenges, such as intellectual property theft, 5G infrastructure policy, and internet governance.

Authorities: The NCD would be added to the statutory list of National Security Council regular attendees. With concurrence from the National Security Advisor or the National Economic Advisor, the NCD would have the capability to convene Cabinet or NSC Principals Committee meetings and the numerous associated preparatory meetings to address cybersecurity and emerging technology issues. Further, the NCD would oversee the compliance of executive departments and agencies with national-level guidance on cybersecurity priorities, strategies, policies, and resource allocations. The NCD will coordinate interagency efforts to defend against adversary cyber operations against domestic U.S. interests; this will not impinge on DoD responsibility for Title 10 activities, Office of the Director of National Intelligence (ODNI) responsibility for Title 50 activities, or the U.S. Department of Justice (DOJ) and Federal Bureau of Investigation (FBI) responsibility for counterintelligence activities, but the NCD would be kept fully apprised of those activities.

The NCD would have budgetary oversight over the cybersecurity community, which is defined as including those areas within the executive branch whose work is critical to the success of the National Cyber Strategy. In the executive branch, each program manager, agency head, and department head with responsibilities under the National Cyber Strategy shall transmit the cyber budget request of the program, agency, or department to the NCD prior to sending it to the Office of Management and Budget (OMB). If the NCD determines that the budget proposed is not in alignment with the National Cyber Strategy, then he or she will recommend appropriate revisions. The NCD's passback revisions must be addressed in the proposed budget and submitted to OMB along with a statement describing the impact of the required budgetary changes on the ability of that program, agency, or department to perform its mission, or, if they cannot be implemented under reasonable circumstances or timelines, what obstacles must be overcome in order to do so. Any significant changes by OMB to the cybersecurity budget of any agency or department would require the concurrence of the NCD.

Resources: The Office of the National Cyber Director would be staffed at a size similar to that of comparable EOP institutions (approximately 50 persons).[160]