THIRD WAY

MEMO *Published September 23, 2021 • 11 minute read*

2021 Reader's Guide to Understanding the Proposed US Cyber Enforcement Budget

Aaron Clarke
Special Advisor to Communications and National Security

Cyber attacks in the United States continue to devastate and disrupt day-to-day operations in the private and public sectors. Marked by events like the ransomware attack on Colonial Pipeline that created gas shortages and increased prices, cybercrime impacts everyday citizens, even if they are not directly targeted by an attack. The Department of Homeland Security (DHS) reported that in 2020 there were "over $4 billion in cybercrime losses reported to the U.S. government." [1] This growing cybersecurity threat has only been exacerbated by the rise of cryptocurrencies like Bitcoin and exposed network vulnerabilities from those working from home during the pandemic. [2]

In response to this influx of cyber attacks, the Biden Administration has taken steps to both bolster the federal government's ability to detect and respond to cyber attacks as well as protect its own systems. [3] The Department of Energy (DOE) and DHS have both made cybersecurity a top priority in their latest initiatives. President Biden called on DOE to launch a 100 day plan aimed at preventing

disrupted services for electric utilities, and DHS announced a series of 60-day "sprints" to support private and public partners against ransomware. [4]

The FY2021 National Defense Authorization Act also created the first U.S. National Cyber Director, tasked to lead the implementation of U.S. cyber policy and strategy, and rapidly improve cybersecurity defense capabilities. Although ransomware attacks have spiked, the federal government has made inroads on combatting cyber criminals. The Cyber Enforcement Budget for FY2022 should continue funding and seek to build on the key improvements and actions taken by the Biden administration.

In this guide, we will look at the budget implications for cyber enforcement, recommendations for Congress, and provide a detailed breakdown of the proposed budget's funding allocations. Specifically, we recommend that Congress should:

- Restore the $15 million of funding cut from the State Homeland Security Program. The program provides critical grants to states that require recipients spend at least 10% of their grants on cybersecurity needs.
- Require an alignment of cybercrime goals and outcomes across law enforcement agencies within the Departments of Homeland Security, Justice, and Treasury.
- Ensure that federal agencies are prepared to implement President Biden's cybersecurity executive order.

The funding for 17 federal agencies tasked with combatting cybercrime equals that of the Defense Department's cyber operations.

In President Biden's proposed budget, roughly $4.4 billion is allocated to 17 civilian agencies and departments to combat cyberattacks and cybercrime, which nearly equals the $4.3 billion solely allocated for the Defense Department's (DOD) cyber operations. [5] The President's proposed budget includes $9.8 billion for all civilian cybersecurity activities, with nearly half devoted to protecting and improving federal IT systems and networks. [6] The remaining $4.3 billion is devoted to providing grants to localities, increasing the resilience of private critical infrastructure, disrupting cybercriminals' computer infrastructure, and investigating and prosecuting cybercriminals. The proposed budget includes new lines of funding, such as standing up the Office of the National Cyber Director, creating a Cyber Response and Recovery Fund, and establishing the Joint Cyber Planning Office. The Administration also increased active civilian defense measures by over $218 million.

Despite this increase, the budgets of these 17 agencies combined nearly equals DOD's cyber operations budget. While the Defense Department engages in offensive operations that disrupt

foreign adversaries' cyber capabilities, state and non-state actors have not been deterred from launching devastating ransomware attacks and other cyber attacks against the United States. Therefore, Congress must ensure that civilian agencies have the commensurate resources to develop resiliency against the inevitable ransomware attacks and establish partnerships with state, local, private, and international stakeholders to hold bad actors accountable.

This must start with the restoration of funding to the State Homeland Security Program. This DHS program provides cybersecurity grants to states and local governments to assist them in bolstering their own cyber capabilities. In the proposed budget, the program saw a $15 million decrease, which means that the 7.5% increase for cyber grants pulls from other priorities. This means that $44.6 million is available in cyber grants for all states, territories, and DC with an average cyber grant of just under $800k. [7]

The decrease in funding combined with the 7.5% allocation to cyber grants comes at a time when state and local governments need significantly more resources to address this increasing threat. Instead of 7.5%, Congress should require that grant recipients spend at least 10% of their grants on cybersecurity needs. This would increase the funding allocated to cybersecurity from $44.6 million to nearly $60 million, with the average cyber grant of just over $1 million. Cybersecurity and cyber enforcement needs will only continue to increase, with state and local governments as frequent targets.[9] Providing additional resources at the state and local level is especially critical when they lack the same defense capabilities as the federal government.

Federal agencies currently lack uniform standards of performance.

The combination of federal agencies tasked with protecting federal networks and the private sector necessitates that they often collaborate with one another. Responding to the Darkside variant of ransomware or providing election security during Super Tuesday required massive collaborative efforts from the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and DHS, among many others. [8] While working together remains integral to ensuring the protection of our networks, each agency carries with it distinct responsibilities, capabilities, and mission statements. Coordination happens at multiple levels across multiple agencies and making sure that these moving parts all work effectively is vital.

Two recent developments have also altered the way that these federal agencies collaborate and coordinate cyber enforcement operations. In November 2018, the Cybersecurity and Infrastructure Security Agency Act was passed and signed into law, creating CISA, an independent federal agency under DHS "in charge of physical and cyber-security of federal networks and critical infrastructure." [9] Since its restructuring from the National Protection and Programs Directorate (NPPD), CISA has quickly seen its authority and budget expanded, especially during the early months of the Biden Administration. On May 12, 2021, President Biden signed an executive order for

CISA to lead and work with other federal agencies on cyber issues like information sharing, detection of cyber incidents, and response coordination. [10]

Even more recently, the Office of the National Cyber Director (NCD) was added within the White House itself. A product of the Cyberspace Solarium Commission, the NCD creates another stakeholder with its own sprawling set of powers. This includes serving as the senior advisor to the President on cyber-related issues, coordinating with federal agencies on responding to cyber attacks, and collaborating and corresponding with the private sector. [11] This also coincides with President Biden's decision to create the position of Deputy National Security Advisor for Cyber and Emerging Technology. [12] This level of coordination on cybersecurity is crucial to combatting bad actors, but unfortunately is not the reality when it comes to standards of performance used to set federal agency budgets.

The President's proposed budget is calculated based on recommendations made by federal agencies. Each agency has their own set of goals and standards of performance that help them determine where funding should go for that respective fiscal year. While this process is typical of all federal agencies, this creates a situation where funds are potentially misaligned and misallocated to handle the collaborative mission of cyber enforcement in the federal government. Most of these federal agencies saw a net increase in their funding for FY22, but that does not necessarily indicate that that funding is appropriately allocated to the nation's overall cyber needs. [13] With specific mandates and authority granted to these federal agencies, an alignment of budgetary needs would correct the current budget process by tying funding to a common mission, rather than separate agencies. By treating the cyber enforcement budget as a singular budget, rather than a collection of individual budgets submitted by each agency, Congress would be better able to isolate and appropriate the necessary resources.

This is especially needed with the rise of CISA and the NCD. As the president's senior advisor on cyber-related issues, the NCD will be responsible for "[reviewing] agency budgets in coordination with the Office of Management and Budget and the NSC" as well as making policy recommendations to those respective agencies. [14] While this authority may serve as a backstop for unnecessary spending within respective agencies, it still creates a piecemeal cyber enforcement budget. With federal agencies still adhering to their own standards of performance, the NCD's review of their respective budgets is unlikely to lead to the necessary realignment of resources.

As the "quarterback" of cybersecurity, CISA has an outsized role in the detection, protection, and response to cyber attacks within the federal government. CISA's "quarterback" role will be at its most effective when their mission, capabilities, and resources are properly aligned across the board. By ensuring that funding is tied to a holistic view of agencies working on cyber enforcement, those conditions can be achieved.

More funding is needed to maximize our return on investment in increased cyber capabilities.

The Biden Administration has made tremendous strides in shining a light onto cybersecurity in the wake of a series of devastating attacks. While the effects of these attacks are still being felt by everyday Americans, the response has been immediate. The culmination of this increased focus came in the form of President Biden's executive order meant to strengthen federal networks and contractors in the event of a cyber intrusion. This sweeping executive action "pushes specific actions to modernize cybersecurity in the federal government, such as zero trust architecture," secure cloud services, and multi-factor authentication among other initiatives. [15] Each agency was given 60 days to update its existing policies around these modernization efforts. The Office of Management and Budget (OMB) and CISA were given 90 days to "develop a Federal cloud-security strategy and provide guidance to agencies accordingly." [16] The pillars set forth in this executive order take crucial steps to securing our federal networks, but implementation may be more difficult if appropriate funding and resources are not set aside.

Problematically, clearly not all federal agencies are starting on equal footing. The DOD's existing infrastructure and budget framework places it in a position to implement these changes more effectively than other agencies who already start off with a smaller budget. These disparities could hinder the uniform implementation across all agencies that is needed to protect the government's systems. There are mechanisms within the executive order that are aimed at correcting this, but those fall short of the mission at hand. The executive order mandates that "based on identified gaps in agency implementation, CISA shall take all appropriate steps to maximize adoption by FCEB [Federal Civilian Executive Branch] Agencies of technologies" for items like multi-factor authentication. [17] While this makes sense with CISA being the government's head cybersecurity agency, it currently faces a daunting task of maximizing these adoptions with static or incomplete funding.

Issues with an agency-by-agency approach to funding complicates any push for modernization. CISA's maximation efforts can only go as far as an agency's budget will allow it, leaving certain agencies and programs worse off or overstretched. This is not to say that CISA would not find ways to work towards closing those gaps, but certain agencies will face a different ceiling on how far those efforts can go. Agencies that do not meet this 180-day goal can "provide a written rationale to the Secretary of Homeland Security through the Director of CISA, the Director of OMB, and the APNSA." [18] This will just leave agencies behind that cannot make up the disparity in the amount of time given with the resources currently allocated to them. The proposed FY22 budget does not account for these changes mandated by the executive order and the pillars within that order will require maintenance and monitoring that currently is not needed. Existing vulnerabilities would be exacerbated if agencies were allowed to fall even further behind. Agencies must be provided necessary funding based on a whole-of-government approach and analysis of cyber threats.

Conclusion

Cybercrime will only continue to rise and the government's cyber capabilities must rapidly progress to meet the challenge. The Biden Administration understands this need and has begun to adjust accordingly with sweeping executive action and a government-wide focus on cybersecurity. This year's proposed cyber enforcement budget seeks to build off this momentum, but Congress needs to ensure that all relevant agencies are properly equipped and funded to protect our government networks. Congress also needs to extract the existing collaborative framework of all relevant cyber enforcement agencies and apply it to the budget process. As everyday Americans feel the burden of cybercrime, it is more crucial than ever for the federal government to take smart and sustained actions.

THIRD WAY

Proposed U.S. Cyber Enforcement Budget FY 2022

Agency and programs
All

Agency and programs	Total for 2022	Increase/decrease from 2021
CISA: Adminstrative Subpeona	$5,000,000.00	$5,000,000.00
CISA: Capacity building	$124,951,000.00	$3,207,000.00
CISA: Cyber excercises	$10,022,000.00	$1,800,000.00
CISA: Cyber response and recovery fund	$20,000,000.00	$20,000,000.00
CISA: CyberSentry	$8,158,000.00	$-??
CISA: Hunt and Incident Response Team	$64,233,000.00	$7,017,000.00
CISA: infrastructure security	$175,300,000.00	Null
CISA: Joint Cyber Planning Office	$10,600,000.00	$10,600,000.00
CISA: National Risk Management Center	$113,928,000.00	$6,652,000.00
CISA: Operational planning and coordination	$79,890,000.00	$10,153,000.00
CISA: stakeholder engagement	$58,180,000.00	$12,455,000.00
CISA: Threat hunting	$158,883,000.00	$(1,568,000.00)
CISA: Vulnerability managment	$144,537,000.00	$(516,000.00)
Commerce: NIST-Cybersecurity and Privacy	$81,900,000.00	$ -
DHS: State Homeland Security Grant Program	$44,601,450.00	$(15,314,000.00)
DOE Cybersecurity, Energy Security, and Emergency Response..	$25,000,000.00	$25,000,000.00
DOE Cybersecurity, Energy Security, and Emergency Response..	$25,000,000.00	$25,000,000.00
DOJ: Criminal Division	$215,173,000.00	$17,919,000.00
DOJ: Economic, high-tech, white collar	$13,000,000.00	$1,000,000.00
DOJ: Intellectual Property Enforcement Program	$2,500,000.00	$-??
DOJ: Interpol Washington	$40,993,000.00	$5,401,000.00
DOJ: National Security Division	$123,093,000.00	$5,642,000.00
EPA	$3,873,000.00	$3,873,000.00
FBI: Cyber investigation resources	$40,000,000.00	$ -
ICE: Homeland Security Investations' Domestic investigation (..	$1,877,754,000.00	$21,821,000.00
IRS: Cybercrimes and applied data analytics	$41,095,000.00	$ -
IRS: enhance enforcement operations	$32,340,000.00	$ -
State: cyber dimplomacy and technology policy	$9,832,000.00	$9,832,000.00
State: INL Cybercrime and IPR	$20,000,000.00	$10,000,000.00
TSA	$3,000,000.00	$ -
USSS: Computer Forensics training	$37,160,000.00	$2,783,000.00
USSS: Domestic and international field operations	$705,391,000.00	$18,808,000.00
USSS: investigative operations	$51,000,000.00	$300,000.00
White House: National Cyber Director	$15,000,000.00	$15,000,000.00

Source: Dille, Grace. "Federal Civilian Cyber Spending Jumps 14% in FY2022 Budget, to $9.8B," *MeriTalk* , https://www.meritalk.com/articles/federal-civilian-cyber-spending-jumps-14-in-fy2022-budget-to-9-8b/, Accessed 10 Sep. 2021.
Environmental Protection Agency. "FY 2022 EPA Budget in Brief," *Environmental Protection Agency* , https://www.epa.gov/sites/default/files/2021-05/documents/fy-2022-epa-bib.pdf, Accessed 10 Sep. 2021.
Federal Bureau of Investigation. "FY 2022 President's Budget Request," *United States Department of Justice,* https://www.justice.gov/jmd/page/file/1399271/download, Accessed 10 Sep. 2021.
Internal Revenue Service. "Budget in Brief," *United States Department of the Treasury,* https://home.treasury.gov/system/files/266/19.-IRS-FY-2022-BIB.pdf, Accessed 10 Sep. 2021.
United States Department of Commerce. "U.S. Department of Commerce FY 2022 Budget in Brief," *United States Department of Commerce,* https://www.commerce.gov/sites/default/files/2021-06/BiB-Final-622-Noon.pdf, Accessed 10 Sep. 2021.
United States Department of Energy. "Department of Energy FY 2022 Congressional Budget Request," *United States Department of Energy,* https://www.energy.gov/sites/default/files/2021-06/doe-fy2022-budget-volume-3.1-v2.pdf, Accessed 10 Sep. 2021.
United States Department of Homeland Security. "FY 2022 Budget in Brief," *United States Department of Homeland Security,* https://www.dhs.gov/sites/default/files/publications/dhs_bib_-_web_version_-_final_508.pdf, Accessed 10 Sep. 2021.
United States Department of Justice. "National Security Division (NSD)," *United States Department of Justice,* https://www.justice.gov/jmd/page/file/1399066/download, Accessed 10 Sep. 2021.
United States Department of Justice. "GENERAL LEGAL ACTIVITIES INTERPOL Washington (USNCB)," *United States Department of Justice,* https://www.justice.gov/jmd/page/file/1399121/download, Accessed 10 Sep. 2021.
United States Department of Justice. "GENERAL LEGAL ACTIVITIES Criminal Division," *United States Department of Justice* , https://www.justice.gov/jmd/page/file/1399001/download, Accessed 10 Sep. 2021.
United States Department of State. "Congressional Budget Justification: Department of State, Foreign Operations, and Related Program," *United States Department of State,* https://www.state.gov/wp-content/uploads/2021/05/FY-2022-State_USAID-Congressional-Budget-Justification.pdf, Accessed 10 Sep. 2021.

TOPICS

CYBERSECURITY 98

ENDNOTES

1. United States Department of Homeland Security. "Secretary Mayorkas Outlines His Vision for Cybersecurity Resilience," *United States Department of Homeland Security,* https://www.dhs.gov/news/2021/03/31/secretary-mayorkas-outlines-his-vision-cybersecurity-resilience, Accessed 10 Sep. 2021.

2. Garcia, Michael and Kristine Johnson. "Digital Currencies' Role in Facilitating Ransomware Attacks: A Brief Explainer," *Third* Way, https://www.thirdway.org/memo/digital-currencies-role-in-facilitating-ransomware-attacks-a-brief-explainer, Accessed 10 Sep. 2021.

   Deloitte, "Impact of COVID-19 on Cybersecurity," *Deloitte,* https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html. Accessed 10 Sep. 2021.

3. Joseph R. Biden Jr. "Executive Order on Improving the Nation's Cybersecurity," *White House,* https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, Accessed 10 Sep. 2021.

4. Garcia, Michael. "What Biden Is Doing on the Other Viral Pandemic," *The Well News,* https://www.thewellnews.com/opinions/what-biden-is-doing-on-the-other-viral-pandemic/, Accessed 10 Sep. 2021.

5. Under Secretary of Defense (Comptroller). "Defense Budget Overview: United States Department of Defense Fiscal Year 2022 Budget Request, *United States Department of Defense,* https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2022/FY2022_Budget_Request_Overview_Book.pdf, Accessed 10 Sep. 2021.

6. Office of Management and Budget. "Analytical Perspectives: Budget of the U.S. Government," *White House,* https://www.whitehouse.gov/wp-content/uploads/2021/05/spec_fy22.pdf, Accessed 10 Sep. 2021.

7. United States Department of Homeland Security. "Department of Homeland Security: Federal Emergency Management Agency Budget Overview," *United States Department of Homeland Security,* https://www.dhs.gov/sites/default/files/publications/federal_emergency_management_agency_0.pdf, Accessed 10 Sep. 2021.

8. Cybersecurity and Infrastructure Security Agency et al. "JOINT STATEMENT FROM DOS, DOJ, DOD, DHS, ODNI, FBI, NSA, AND CISA ON PREPARATIONS FOR SUPER TUESDAY," *Cybersecurity and Infrastructure Security Agency,* https://www.cisa.gov/news/2020/03/02/joint-statement-dos-doj-dod-dhs-odni-fbi-nsa-and-cisa-preparations-super-tuesday, Accessed 10 Sep. 2021.

   Cybersecurity and Infrastructure Security Agency and the Federal Bureau of Investigation. "Joint CISA-FBI Cybersecurity Advisory on DarkSide Ransomware," *Cybersecurity and Infrastructure Security Agency,* https://us-cert.cisa.gov/ncas/current-activity/2021/05/11/joint-cisa-fbi-cybersecurity-advisory-darkside-ransomware, Accessed 10 Sep. 2021.

9. Cimpanu, Catalin. "Trump signs bill that creates the Cybersecurity and Infrastructure Security Agency," *ZD Net*, https://www.zdnet.com/article/trump-signs-bill-that-creates-the-cybersecurity-and-infrastructure-security-agency/, Accessed 10 Sep. 2021.

10. Cybersecurity and Infrastructure Security Agency. "EXECUTIVE ORDER ON IMPROVING THE NATION'S CYBERSECURITY," *Cybersecurity and Infrastructure Security Agency*, https://www.cisa.gov/executive-order-improving-nations-cybersecurity, Accessed 10 Sep. 2021.

11. Costello, John and Mark Montgomery. "How the National Cyber Director Position Is Going to Work: Frequently Asked Questions," *The Lawfare Institute,* https://www.lawfareblog.com/how-national-cyber-director-position-going-work-frequently-asked-questions, Accessed 10 Sep. 2021.

12. Dille, Grace. "Biden Picking Two Cyber Experts for Top DoJ, NSC Posts," *MeriTalk,* https://www.meritalk.com/articles/biden-picking-two-cyber-experts-for-top-doj-nsc-posts/, Accessed 10 Sep. 2021.

13. United States Department of Homeland Security. "Department of Homeland Security: Federal Emergency Management Agency Budget Overview," *United States Department of Homeland Security,* https://www.dhs.gov/sites/default/files/publications/federal_emergency_management_agency_0.pdf, Accessed 10 Sep. 2021.

14. Costello, John and Mark Montgomery. "How the National Cyber Director Position Is Going to Work: Frequently Asked Questions," *The Lawfare Institute,* https://www.lawfareblog.com/how-national-cyber-director-position-going-work-frequently-asked-questions, Accessed 10 Sep. 2021.

15. Joseph R. Biden Jr. "Executive Order on Improving the Nation's Cybersecurity," *White House,* https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, Accessed 10 Sep. 2021.

16. Joseph R. Biden Jr. "Executive Order on Improving the Nation's Cybersecurity," *White House,* https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, Accessed 10 Sep. 2021.

17. Joseph R. Biden Jr. "Executive Order on Improving the Nation's Cybersecurity," *White House,* https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, Accessed 10 Sep. 2021.

18. Joseph R. Biden Jr. "Executive Order on Improving the Nation's Cybersecurity," *White House,* https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, Accessed 10 Sep. 2021.