Botnet Road Map
Status Update

Prepared by
The Departments of
Commerce and Homeland Security

July 28, 2020

Certain commercial equipment, instruments, or materials are identified in this paper in order to adequately characterize progress implementing the road map. Such identification is not intended to imply recommendation or endorsement by the Departments of Commerce or Homeland Security, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

Table of Contents

I. Background

On May 11, 2017, the President issued Executive Order (EO) 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," calling for "resilience against botnets and other automated, distributed threats."[1] The President directed the Secretaries of Commerce and Homeland Security to "lead an open and transparent process to identify and promote action by appropriate stakeholders" with the goal of "dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets)."[2]

The Departments of Commerce and Homeland Security worked jointly on the effort, publishing the report on *Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*, known as the *Botnet Report*, in May 2018.[3] Based on input from stakeholders across industry and government, the report called for the federal government to clearly delineate priorities for action. The initial Botnet Road Map (road map), published in November 2018, laid out actions that could dramatically reduce the threat of botnets and similar attacks, consistent with Administration priorities as set forth in the National Cyber Strategy.[4,5]

The road map recognized that the botnet challenge will not be resolved quickly. This as an ecosystem-wide problem that requires sustained collaboration across industry, government, academia, and civil society. By indicating its priorities, the federal government can increase stakeholder confidence that resources invested in industry-led actions with federal dependencies will result in productive outcomes.

This document provides a status update on efforts across the ecosystem to enhance the resilience of the Internet against distributed, automated attacks. This update was mandated by the road map itself. In this document:

- Section II offers a reassessment of the threat of automated, distributed attacks;
- Section III reviews progress the community as a whole is making in the areas highlighted by the road map and the impacts of those activities;
- Section IV provides an update on the President's National Security Telecommunications Advisory Committee's (NSTAC) Report to the President on a Cybersecurity Moonshot,[6] as referenced in the Botnet Report;[7] and

---

[1] Exec. Order No. 13800, 82 Fed. Reg. 22,391, at 22,394 (May 11, 2017), *available at* https://www.federalregister.gov/d/2017-10004.
[2] *Id.*
[3] U.S. Dep't of Commerce & U.S. Dep't of Homeland Sec., *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*, (May 2018), *available at* https://www.commerce.gov/sites/default/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf.
[4] U.S. Dep't of Commerce & U.S. Dep't of Homeland Sec., *A Road Map Toward Resilience Against Botnets* (Nov. 2018), *available at* https://www.commerce.gov/sites/default/files/2018-11/Botnet%20Road%20Map%20112918%20for%20posting_1.pdf
[5] Nat'l Sec. Council, *National Cyber Strategy of the United States of America*, (Sept. 2018), *available at* https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
[6] Nat'l Sec. Telecomms. Advisory Comm., *NSTAC Report to the President on a Cybersecurity Moonshot* (Nov. 14, 2018), *available at* https://www.cisa.gov/sites/default/files/publications/NSTAC_CyberMoonshotReport_508c.pdf.
[7] The effort described in Section IV was not explicitly discussed in the road map, but was featured in the *Botnet Report*, and was included in this update for completeness.

- Section V identifies important activities that lie ahead in the coming year.

Development Process

This document reviews ongoing efforts by government, civil society, technologists, academics, and industry sectors to enhance the resilience of the Internet against botnets. The review is organized according to the five lines of effort described in the Botnet Report, focusing largely on the tasks identified in the associated road map. The Botnet Report and the road map were developed using an open and transparent process, and reflect a general consensus among the community. The purpose of this status report is to determine if the community as a whole is making sufficient progress mitigating botnets.

For this assessment, data was gathered through an informal process, leveraging contacts in agencies and the private sector established during the development of the Botnet Report and road map. Relevant projects have been identified throughout this document to support our assessment of progress within each line of effort. Given the process, those projects are largely drawn from the road map itself. Since a public review period was not conducted, it is likely that other relevant efforts are also underway in addition to those noted in this document. Identification of a project in this document does not imply an endorsement by the Departments of Commerce or Homeland Security, and the reader should not assume that projects identified within this document are the best, much less only, efforts in a particular space.

II. Re-Assessing the Threat of Botnet Attacks

The Department of Homeland Security commissioned two research reports on botnet attacks: *Technical Options and Approaches for Implementing Botnet Recommendations*, and *Targeting Trends for Botnet Growth*. These reports were reviewed to determine whether significant course changes in the overall effort were warranted.

Collectively, the two reports suggest that botnets will continue to be a threat for the foreseeable future, and in largely predictable fashion. Perhaps the most surprising assessment is the forecast of smaller, rather than larger, botnets. Given that the report predicts a continued increase in botnet "power," this offers little comfort. It seems clear that the urgency of mitigating botnet attacks expressed in Executive Order 13800 is still warranted.

Report Excerpt: Technical Options and Approaches for Implementing Botnet Recommendations

"It seems likely, based on historical behaviors, that:

- *Botnets will continue to **grow in sophistication** in order to counter efforts to disrupt them. This will likely include developing new techniques to evade detection, secure command and control, and increase overall resiliency of the botnet.*
- *Botnets will **expand to utilize new types of connected devices**. This will likely lead to even more types of consumer IoT products being coopted into botnets, and potentially greater utilization of mobile/wearable devices and other classes of IoT (such as industrial devices).*

- *The **malicious operations will be enhanced and extended**. Representing the objectives to which botnets are put (e.g., spam campaigns, denial of service, etc.), botnet authors will try to find ways to enhance the effectiveness of these actions and will also be on the lookout for new uses to which to put their botnets.*
- ***Social media botnets** are likely to see continued use and development, both as a means of making money off the social media user community and as a way to try to influence the opinions and politics of these communities.*
- *Finally, it is likely that an increasing number of state actors will see operations in cyberspace as a means to further their national agendas and will see botnets as a powerful tool towards those ends. This **state sponsorship of botnet development** will result in new innovations, but those innovations will almost inevitably end up captured, dissected, and re-purposed by criminal enterprises."*[8]

Report Excerpt: Targeting Trends for Botnet Growth

"[There are] three important implications for global botnet behavior that arise from trends in botnet targeting practices: botnet sizes, global distribution patterns, and drivers of target expansion:

- ***Botnet Size**—One might imagine that more connected devices would mean botnets would grow ever larger, but this does not appear to be the case. In fact, there appear to be multiple factors that limit the size of modern botnets, including limited targets, competition from other botnets, and the desire to avoid triggering coordinated responses by defenders. While it is true that botnets are growing ever more powerful (as evidenced by the steady increase in the magnitude of Distributed Denial of Service (DDoS) attacks), that seems to have more to do with better tools and techniques than raw size.*
- ***Global Distribution**—Botnets tend to have uneven global distribution. Often this is the unintentional impact of targeting certain makes and models of devices – regions where those devices have greater market penetration will naturally see greater instances of infection. In other cases, botnet authors will sometimes deliberately target or avoid certain regions, usually driven by operational concerns. Similarly, botnet authors might be more familiar with certain languages and cultures and since email remains a common vector for bot malware distribution, this familiarity can lead to greater conversion rates of those messages into bot infections. By contrast, botnet operators have been seen to avoid infections in certain regions, often to avoid the attention of law enforcement in the region in which the botnet operators physically reside.*
- ***Drivers of Target Expansion**—While devices and device classes might differ in their ability to support a given type of malicious botnet campaign, overall botnet operators don't appear to spend much effort avoiding less useful devices. Observation of current botnets seems to suggest that virtually any compromised device is seen as having some benefit by a botnet operator, and if the opportunity for compromise is there, the botnet operator usually takes*

[8] Homeland Sec. Sys. Eng'g & Dev. Inst., U.S. Dep't of Homeland Sec., *Technical Options and Approaches for Implementing Botnet Recommendations: Botnet Bestiary Report* (June 24, 2019).

it. At the same time, different botnets often end up competing with each other for resources. Certain popular software products with known vulnerabilities are often targeted by multiple botnets, and botnets have been seen removing competing bots and even patching systems once they have installed their own malware to prevent other botnets from gaining access. Both of these factors incentivize botnet authors to explore compromises of new devices and further broaden the field of botnet targets."[9]

III. Progress Against Road Map and Impact by Line of Effort

The road map laid out tasks related to each action in the context of five lines of effort:

1. Internet of Things (IoT);
2. Enterprise;
3. Internet Infrastructure;
4. Technology Development and Transition; and
5. Awareness and Education.

While each task is incremental in nature, they are all mutually supportive and, in aggregate, will contribute to a more resilient Internet. Some tasks are the direct responsibility of the federal government, while others are specific to the private sector. Certain tasks do not directly involve the federal government, but support, or are supported by, actions that depend on federal involvement or leadership.

As explained in the road map, the U.S. government values innovation, and expects the market to determine the most expeditious solutions to the identified concerns. This is why the tasks in the road map were not direct assignments. The lines of effort were designed to be flexible, and as expected, the progress made did not always align directly with road map tasks. We welcome continued creativity and innovation in addressing the botnet challenge.

This section gives a broad overview of the progress since the publication of the road map, highlighting some key success stories in each line of effort. Coverage of activities within the federal government is most comprehensive. Activities underway in private sector consortia and standards activities are often public knowledge, and are included where known. We have less visibility into activities underway within private enterprises, so product development and privately funded research activities are likely underrepresented.

Internet of Things Line of Effort

The Botnet Report recognized that connected devices can extend the scope and scale of automated, distributed attacks. The IoT Line of Effort focuses on reducing security risk across the IoT ecosystem through the establishment and adoption of baseline security standards applied across the full lifecycle of IoT devices.

While IoT devices are broadly considered insecure, there has historically been little agreement on what level of security functionality is needed for a particular device. This line of effort seeks to establish consensus on security capability baselines for three sectors: consumers/home users, industrial users,

[9] Ibid.

and the federal government. The road map envisions contributions from the public and private sectors, followed by development of international standards, and culminating in a set of supporting activities designed to develop a robust market for conforming products.

This line of effort also includes a portfolio of actions to enhance the security of IoT products and promote confidence in the IoT marketplace, independent of the three sector-specific security baselines. Tasks focus on collaboration between cybersecurity and operational technology communities, and international policy advocacy, harmonization, and standards. With the exception of developing globally relevant IoT standards, these activities have few dependencies. A key challenge will be prioritizing activities to reflect resource availability.

The following highlights demonstrate significant progress in this line of effort. In particular, the public and private sectors have contributed initial capability baselines, and consensus baselines are emerging. More recently, the initiation of new international standards efforts bodes well for the development of globally relevant IoT standards.

Highlights

Since the publication of the 2018 Botnet Report, the National Institute of Standards and Technology (NIST) has hosted a series of public workshops, webinars, and industry roundtables on IoT cybersecurity, and is participating in or monitoring a number of U.S. industry and international efforts. NIST has issued a series of publications on IoT cybersecurity to serve the full range of stakeholders, including manufacturers, businesses, and consumers. Future publications in this series will include federal IoT security baselines, which will enable government-wide or department-specific procurement efforts. The NIST baselines also provide a foundation for contributions to international consensus baselines, such as the ongoing work in the International Organization for Standardization (as described on the following page). Relevant milestones include:

- NIST finalized the introductory document, NIST Interagency Report (NISTIR) 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, in June 2019.[10] This publication helps federal agencies and other organizations better understand and manage the cybersecurity and privacy risks associated with use of IoT devices and establishes the foundation for publications on more specific aspects of IoT security. (Action 1.1)

- NIST continued publication of the series with the second draft of NISTIR 8259: Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline in January 2020.[11] This draft publication defines a core baseline of cybersecurity capabilities that manufacturers can voluntarily adopt for IoT devices they produce—a foundational element of the road map's IoT Line of Effort. It also provided information on how manufacturers can identify and implement capabilities beyond the core baseline most appropriate for their customers. The comment period for second draft NISTIR

[10] Katie Boeckl et al., C*onsiderations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* (June 2019), NIST Interagency/Internal Report No. 8228, *available at* https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf.
[11] Michael Fagan et al., *Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline* (Jan. 2020), (NIST Interagency/Internal Report No. 8259 (Second Draft)), *available at* https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259-draft2.pdf.

8259 closed February 7, 2020, and NIST is currently resolving comments with a goal of final publication in mid-2020. (Action 1.1)

- Draft NISTIR 8267, Security Review of Consumer Home IoT Products, is another addition to the series.[12] The report summarizes findings from a review of connected devices and details a series of considerations to manufacturers for improving security of home IoT products. These considerations were developed through open-source research, hands-on review, and security capabilities analysis of several commonly purchased IoT consumer home devices. NIST plans to build on this foundation through follow-on projects and documents. The comment period for Draft NISTIR 8267 closed November 1, 2019. (Action 5.1)

NIST's National Cybersecurity Center of Excellence (NCCoE) is collaborating with industry to demonstrate effective mitigation of IoT-based DDoS attacks using the manufacturer usage description (MUD) defined in Internet Engineering Task Force (IETF) Request for Comments (RFC) 8520.[13] Using MUD, the network can automatically restrict the IoT device to required communication paths. That is, the network will prohibit all other device behaviors, limiting the IoT device's attack surface and preventing attacks by compromised devices. The NCCoE released the initial draft version of the NIST Cybersecurity Practice Guide Special Publication 1800-15 on mitigating IoT-based DDoS in April 2019 and an updated draft in November 2019.[14] The practice guide details the use of MUD for commercial and open source implementations. (Action 1.4)

The NCCoE and its industry collaborators also organized a MUD-focused hackathon at the IETF's July 2019 meeting to advance the pace of maturation and adoption of RFC 8520. By sharing practical implementations of the MUD technology with other IETF participants and collaborating on development of open source solutions, the hackathon promoted adoption and extension of the MUD specification. (Action 1.4)

From the private sector, the Council to Secure the Digital Economy (CSDE) released the C2 Consensus on IoT Device Security Baseline Capabilities (C2 Consensus Baseline) in September 2019.[15] The industry-led C2 project incorporated input from dozens of technical experts across an international spectrum to develop a common set of security capabilities that can be applied to new IoT devices. It lays out key baselines, designed to be flexible, for optional use by manufacturers and any others that are seeking out guidance. The baselines, identified as complementary in the Botnet Road Map to NISTIR 8259, focus on secure device capabilities and product lifecycle management capabilities, with an emphasis on customizing an organization's baseline to the needs of the specific device. (Action 1.1)

---

[12] Michael Fagan et al., *Security Review of Consumer Home Internet of Things (IoT) Products* (Oct. 2019) (NIST Interagency/Internal Report No. 8267 (Draft)), *available at* https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8267-draft.pdf.

[13] E. Lear et al., *Request for Comments No. 8520: Manufacturer Usage Description Specification* (Mar. 2019) (Draft), Internet Eng'g Task Force, *available at* https://tools.ietf.org/html/rfc8520.

[14] Donna Dodson et al., *Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)* (Nov. 2019) (NIST Special Publ'n 1800-15 (Second Preliminary Draft)), *available at* https://www.nccoe.nist.gov/publication/1800-15/.

[15] Council to Secure the Dig. Econ., *The C2 Consensus on IoT Device Security Baseline Capabilities* (Sept. 2019), *available at* https://www.tiaonline.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf.

Commercial baselines are also under development through a variety of industry forums. One notable example is GlobalPlatform's IoTopia Committee, which first met in October 2019. The IoTopia Committee is developing technical specifications for security and interoperability. These specifications build upon industry standards, such as MUD, to establish four foundational pillars for IoT device security: 1) security by design; 2) device intent; 3) autonomous, scalable, secure onboarding; and 4) device lifecycle management.[16] (Action 1.1)

IoT-focused standards efforts are ongoing in several international bodies, including efforts that would extend and enhance MUD-based network security. The IETF has nearly completed work on the Bootstrapping Remote Secure Key Infrastructures (BRSKI)[17] standard for secure onboarding and increased assurance for device identification. The Wi-Fi Alliance's Device Provisioning Protocol (DPP) specification[18] defines a framework for user friendly setup in Wi-Fi environments, and may be extendable to other environments. Equally important are nascent efforts to standardize access to MUD files for Fifth Generation (5G) connected IoT devices now underway in the Third Generation Partnership Project (3GPP).[19] (Actions 1.1, 1.2)

A proposal to begin work on an international standard, "Cybersecurity - IoT Security and Privacy - Device baseline requirements," was approved by the working group in a joint technical committee of the International Organization for Standardization and the International Electrotechnical Commission known as ISO/IEC JTC 1 Standards Committee 27, and will be moving to ballot to approve.[20] While such processes take time, this process may lead to an international standard for baseline requirements for IoT devices to support information security and privacy controls. (Action 1.2)

The nonprofit Global Cyber Alliance continued to add to its existing suite of free cybersecurity tools, launching its Automated IoT Defence Ecosystem (AIDE).[21] AIDE is automatically collecting IoT attack data from honeyfarms, virtual IoT devices on simulated networks, and proxypots, and is aggregating that data into an analysis platform available for researchers to study IoT attack signatures and patterns. The platform generates data feeds that are widely available across the Internet ecosystem to mitigate IoT attacks. AIDE also allows an edge router or other policy enforcement point to use threat feeds to mitigate attacks against the local environment, using an application of the MUD standard. (Action 1.4)

Enterprise Line of Effort

The Enterprise Line of Effort is focused on those actions that can be taken at the enterprise management level to reduce the overall risk to the enterprise and the ecosystem from botnets and other automated, distributed attacks.

---

[16] *GlobalPlatform Launches Comprehensive Approach to IoT Cybersecurity Implementation* (Oct. 23, 2019), https://globalplatform.org/latest-news/globalplatform-launches-comprehensive-approach-to-iot-cybersecurity-implementation/ (last visited Feb. 14, 2020).
[17] M. Pritikin et al., *Bootstrapping Remote Secure Key Infrastructures (BRSKI)* (Mar. 26, 2018) (Internet Draft), Internet Eng'g Task Force, *available at* https://tools.ietf.org/id/draft-ietf-anima-bootstrapping-keyinfra-13.html.
[18] Wi-Fi Alliance, *Device Provisioning Protocol Specification: Version 1.1* (2018), *available at* https://www.wi-fi.org/download.php?file=/sites/default/files/private/Device_Provisioning_Protocol_Specification_v1.1_0.pdf.
[19] *See* 3GPP, *available at* https://www.3gpp.org/ (last visited Feb. 3, 2020).
[20] Relevant Working Group documents are not yet available but are anticipated to be available at https://www.iso.org/committee/45306/x/catalogue/p/0/u/1/w/0/d/0.
[21] Global Cyber Alliance, *AIDE: Automated IoT Defence Ecosystem*, *available at* *https://www.globalcyberalliance.org/aide/* (last visited Dec. 9, 2019).

It includes activities to help enterprises that have embraced the NIST Cyber Security Framework (CSF) to mitigate DDOS attacks and protect against botnets, promote migration to more robust and defensible network architectures, encourage federal adoption of industry best practices, and enhance the security of operational technology (OT) devices.

Since publication of the road map, the private sector has contributed CSF profiles for mitigation and protection against DDOS attacks and botnets in general, research in advanced enterprise network architectures is underway including several notable public/private collaborations, and public-private working groups were established to promote secure deployment of OT devices.

Highlights

In early 2019, the Cybersecurity Coalition finalized its DDoS and Botnet Threat Mitigation Profiles for the NIST Cybersecurity Framework. The DDoS Threat Mitigation Profile[22] focused on using the Cybersecurity Framework to improve organizational defenses and responses to DDoS attacks, while the Botnet Threat Mitigation Profile[23] focused on reducing the likelihood of devices becoming part of a botnet and mitigating the situation for devices that have. (Action 2.2)

The NCCoE is also partnering with the Federal CIO Council, Department of Defense, and other agencies to evaluate zero trust networking capabilities. Using knowledge gained in this NCCoE demonstration project, NIST published Draft SP 800-207, Zero Trust Architecture, in September 2019 and updated the document in February 2020.[24] Related NCCoE efforts include Domain Name System (DNS)-based secure electronic mail and an examination of micro segmentation in ongoing energy sector security projects. (Action 3.3)

The Department of Homeland Security (DHS) issued Binding Operational Directive (BOD) 19-02, Vulnerability Remediation Requirements for Internet-Accessible Systems, which introduces a shorter timeframe for agencies to mitigate critical vulnerabilities and a new timeframe for mitigation of high-severity flaws.[25] These steps will reduce the overall attack surface of federal civilian networks and lower the risk of unauthorized access to federal information systems. (Action 1.3)

CSDE published its International Anti-Botnet Guide in late 2018, focusing on voluntary participation and collaboration among disparate stakeholders throughout the global Internet and communications ecosystem.[26] The guide highlighted voluntary practices for each segment of the Information and Communications Technology (ICT) sector, ranging from "baseline" to "advanced." Many of the practices

---

[22] Cybersecurity Coalition, *Cybersecurity Framework: DDoS Threat Mitigation Profile*, *available at* https://www.cybersecuritycoalition.org/ddos-framework (last visited Dec. 9, 2019).
[23] Cybersecurity Coalition, *Cybersecurity Framework: Botnet Threat Mitigation Profile*, *available at* https://www.cybersecuritycoalition.org/botnet-framework (last visited Dec. 9, 2019).
[24] Scott Rose et al., *Zero Trust Architecture* (Feb. 2020), NIST Special Publ'n 800-207 (2nd Draft), *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf.
[25] Cybersecurity & Infrastructure Sec. Agency, U.S. Dep't of Homeland Sec., *Binding Operational Directive 19-02: Vulnerability Remediation Requirements for Internet-Accessible Systems* (Apr. 29, 2019), *available at* https://cyber.dhs.gov/assets/report/bod-19-02.pdf.
[26] Council to Secure the Dig. Econ., *International Anti-Botnet Guide 2018* (Nov. 2018), *available at* https://securingdigitaleconomy.org/wp-content/uploads/2018/11/CSDE-Anti-Botnet-Report-final.pdf.

and technologies discussed in the guide are already being used by large-scale enterprises, but the guide aims to spur wider implementation of these capabilities. In November 2019, the council published its International Botnet and IoT Security Guide 2020, updating the 2018 guide with a discussion of how the threat has evolved, and incorporating input from the C2 Consensus Baseline discussed above.[27] (Actions 3.1, 3.3)

In the OT area, a working group of stakeholders from Department of Defense (DoD), International Society of Automation (ISA), and National Electrical Manufacturers Association (NEMA) have proposed a program to apply industry-accepted standards to improve safety and security of currently vulnerable building control system processes, products, and technologies. This program will review and integrate existing international standards with industry best practices to promote the use of a tiered security posture for the building management system, selected by the end user, based on risk to a facility or operation. It addresses the entire value chain of a building control system and is confirmed via regular third-party control system enterprise and process evaluations.[28] In June 2019, the working group solicited feedback on its prospectus framework document for the new program from the wider stakeholder community, and reported a favorable response. The working group will soon present this program directly to the end user community. (Action 4.5)

DHS/the Cybersecurity and Infrastructure Security Agency (CISA) continues to host the Industrial Control Systems Joint Working Group (ICSJWG) to facilitate information sharing and reduce the risk to the nation's industrial control systems among asset owners, operators, integrators, private industry, government, state, local, tribal, territorial, and academic partners in the industrial control system (ICS) community.[29] The bi-annual meetings comprised of keynotes, presentations, panels, demonstrations, and a technical workshop provide an opportunity for stakeholders to network, hear from industry leaders, and stay abreast of the latest initiatives impacting ICS security and the nation's critical infrastructure. The ICSJWG offers a technical workshop throughout the three-day event, providing hands-on training and insight into usable toolkits, analytics, forensics, and techniques. (Action 4.5)

DHS/CISA is also leading the Control Systems Interagency Working Group (CSIWG), intended to highlight OT and control system concerns and design solutions in conjunction with the private sector. The group has identified workforce development, supply chain risk management, incident management, and standards as four areas that will require a close public-private partnership approach to attain success. It is currently working on a national strategy and implementation plan to address control systems. The group is also establishing a formal feedback channel with industry for future collaboration. (Action 4.5)

Infrastructure Line of Effort

The Infrastructure Line of Effort focuses on actions that will require coordination across the vast diversity of digital ecosystem players, or that impact the core functional capabilities of the global digital infrastructure. This line of effort envisioned improvements to routing security, increased information

[27] Council to Secure the Dig. Econ., *International Botnet and IoT Security Guide 2020* (Nov. 2019), *available at* https://securingdigitaleconomy.org/wp-content/uploads/2019/11/CSDE_Botnet-Report_2020_FINAL.pdf.
[28] *NEMA, ISA Announce New Building Systems Cybersecurity Program* (May 23, 2019), https://www.nema.org/news/Pages/NEMA,-ISA-Announce-New-Building-Systems-Cybersecurity-Program.aspx (last visited Feb. 14, 2020).
[29] Industrial Control Systems Joint Working Group (ICSJWG), https://www.us-cert.gov/ics/Industrial-Control-Systems-Joint-Working-Group-ICSJWG (last visited Feb. 14, 2020).

sharing in practice, more efficient information sharing protocols, and focused research and development.

Since publication of the road map, new information sharing organizations have been established by the private sector as well as government-organized public-private collaborations, protocols for efficient information sharing during DDoS attacks have been published, and industry has developed playbooks for cyber crisis communication. Best practices have been documented and legal impediments identified. Finally, hundreds of Internet infrastructure providers are coalescing behind a set of routing security principles.

Highlights

The 2018 Botnet Report highlighted the importance of information sharing to accelerate and enhance the effectiveness of botnet identification and mitigation. Significant progress has been achieved since publication of the report, both within government and private industry, including the following activities and milestones:

- On November 16, 2018, the President enacted the Cybersecurity and Infrastructure Security Agency Act of 2018 establishing CISA.[30] A large part of CISA's activity involves continuing and expanding DHS' previous efforts to promote and enable timely and effective sharing of cybersecurity information among public and private entities across all critical infrastructure sectors. Key information-sharing initiatives that fall under the CISA purview include the DHS Cyber Information Sharing and Collaboration Program (CISCP), National Cybersecurity and Communications Integration Center's (NCCIC's) operation as a global exchange for cyber and communications information, and the establishment and coordination of information sharing and analysis organizations (ISAOs), which were initiated by Presidential Executive Order 13691 to enable organizations that fall outside of the sectors served by information sharing and analysis centers (ISACs) to participate in similar sharing of cybersecurity information.[31] DHS continues to support these important initiatives as a key part of its mission. (Action 2.4)

- In the area of automated information sharing, the IETF published RFC 8612, DDoS Open Threat Signaling (DOTS) Requirements, which describes the required characteristics of protocols to enable automated sharing of DDoS information by incident responders.[32] The IETF is also working on a complementary architecture and data specification for DOTS. Together, the standard, architecture, and data specification will define a standardized method for network operators to use in coordinating a real-time response to DDoS and to increase the effectiveness of their efforts to mitigate DDoS attacks' impacts. (Action 2.1)

- Industry is also exploring automated information sharing processes to enhance the timeliness and value of shared threat information. For example, the Cyber Threat Alliance's 23 members

[30] Cybersecurity & Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, 132 Stat. 4168 (2018), *available at* https://www.congress.gov/bill/115th-congress/house-bill/3359/text.
[31] Exec. Order No. 13691, 80 Fed. Reg. 9,347–9,353 (Feb. 13, 2015), *available at* https://www.federalregister.gov/documents/2015/02/20/2015-03714/promoting-private-sector-cybersecurity-information-sharing.
[32] A. Mortensen et al., *Request for Comments No. 8612: DDoS Open Threat Signaling (DOTS) Requirements*, (May 2019), Internet Eng'g Task Force, *available at* https://tools.ietf.org/html/rfc8612.

share about 13 million artifacts, many with supporting context and analysis, each quarter.[33] The Cyber Threat Alliance uses an automated platform based on Structured Threat Information eXpression (STIX) data interchange format to expedite processing and reduce the detection-to-deployment lifecycle. (Actions 4.1, 4.4)

- CSDE released a report titled *Cyber Crisis: Foundations of Multi-Stakeholder Coordination*, which contains a blueprint for industry coordination in the event of a cyber crisis such as a massive botnet attack.[34] The report considers strategies for a total of 12 significant cybersecurity events, including a DDoS botnet attack. The report noted that response strategies should be framed in the context of voluntary frameworks where industry leads decisively, leveraging the mature assets and capabilities of ICT companies. (Actions 4.1, 4.4)

The 2018 Botnet Report also highlighted a need for deployment of existing but underutilized technologies to increase the resilience and agility of our network infrastructure. Recommendations for best practices and technical specifications addressing these requirements were released in the past year. Examples include:

- In December 2019, NIST released the final version of NIST SP 800-189, Resilient Interdomain Traffic Exchange—BGP Security and DDoS Mitigation.[35] This document provides technical guidance and recommendations for deploying technologies that improve the security of interdomain traffic exchange. It focuses on securing the interdomain routing control (i.e., Border Gateway Protocol [BGP]) traffic as well as mitigating DDoS attacks. This document applies to enterprise networks and the network services of hosting providers (e.g., cloud-based applications and service hosting) and Internet service providers (ISPs) that support them. Final publication of SP 800-189 is expected early in 2020. (Action 3.3)

- Through collaborative efforts with industry at the National Cybersecurity Center of Excellence, NIST is evaluating emerging technologies and best practices for incorporation into the Cybersecurity Framework. Examples include the recently completed Secure Inter-Domain Routing project[36] and the ongoing Security for IoT Sensor Networks project.[37] The Secure Inter-domain Routing project used commercially available technologies to demonstrate the practicality of BGP Route Origin Validation, which leverages the Resource Public Key Infrastructure (RPKI) to address and resolve the erroneous exchange of network routes. Several organizations with relevant capabilities have agreed to collaborate with NIST in a consortium to build this example solution. (Action 3.3)

---

[33] *See* Cyber Threat Alliance, *available at* https://www.cyberthreatalliance.org/ (last visited Feb. 3, 2020).
[34] Council to Secure the Dig. Econ., *Cyber Crisis: Foundations of Multi-Stakeholder Coordination* (Sept. 2019), *available at* https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_CyberCrisis-Report_2019-FINAL.pdf.
[35] Kotikalapudi Sriram & Doug Montgomery, *Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation* (Dec. 2019), NIST Special Publ'n 800-189, *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-189.pdf.
[36] Nat'l Cybersecurity Ctr. of Excellence, Nat'l Inst. of Standards & Tech., *Secure Inter-Domain Routing*, *available at* https://www.nccoe.nist.gov/projects/building-blocks/secure-inter-domain-routing (last visited Dec. 9, 2019).
[37] Nat'l Cybersecurity Ctr. of Excellence, Nat'l Inst. of Standards & Tech., *Security for IoT Sensor Networks*, *available at* https://www.nccoe.nist.gov/projects/building-blocks/iot-sensor-security (last visited Dec. 10, 2019).

- In January 2019, the University of Pennsylvania published the results of a yearlong investigation into the hypothesis that legal issues pose barriers to RPKI adoption.[38] The report evaluates the issues raised by community members and proposes several strategies to reduce or circumvent material barriers. The research, supported by the National Science Foundation (NSF), was also the subject of extensive discussions at the Spring 2019 American Registry for Internet Numbers (ARIN) meeting. ARIN is actively looking into a number of ways to make RPKI workable throughout the region, particularly by reducing and managing liability risks. The report noted specific impediments faced by federal agencies that complicate signing the RPKI Relying Party Agreement and Registration Services Agreement. ARIN has agreed to waive problematic provisions in both agreements, including indemnification and choice of law clauses, and is reviewing several other provisions. In aggregate, these changes may create a path for federal agencies to obtain RPKI certificates for their autonomous system numbers, improving the security of the global routing system writ large. (Action 2.3)

- In March 2019, the Communications Security, Reliability, and Interoperability Council (CSRIC) of the Federal Communications Commission (FCC) published its *Final Report on Best Practices and Recommendations to Mitigate Security Risks to Current IP-Based Products*.[39] CSRIC VI, Working Group 3, examined the findings of the previous CSRICs to understand how those findings aligned with today's current DNS, and whether there were new issues that should be addressed. New best practices are coming to fruition to address many issues remaining in DNS and BGP (as well as other Internet protocols and applications). The report identified a need for future studies of the DNS and its routing protocol BGP, to ensure that the system is made more secure without impacting performance. (Action 2.5)

The 2018 Botnet Report also highlighted the need to measure routing security and encourage adoption by network operators. The Mutually Agreed Norms for Routing Security (MANRS) initiative launched the MANRS Observatory in August 2019.[40] The online tool measures the level of networks' compliance with MANRS, which is a key indicator of the state of routing security and resilience of the Internet. It aggregates data from trusted third-party sources into a dashboard, enabling network operators to identify problem areas to help them improve the security of their networks. In addition, as of September 2019, more than 200 network operators or operators of Internet exchange points had signed on to participate in the MANRS global routing security initiative. (Action 2.5)

Technology Development and Transition Line of Effort

This line of effort focuses on establishing a robust and sustainable market for systems and applications developed through secure software development practices. Tasks establish widely accepted guidelines for secure software development, increase the efficiency and effectiveness of tools for secure software development to increase return on investment, and showcase these advances in government-sponsored technology forums. It includes international coordination on standards development and promotion of best practices, as well as an increased focus on research and development.

---

[38] Christopher S. Yoo & David A. Wishnick, *Lowering Legal Barriers to RPKI Adoption*, Fac. Scholarship Penn L. 2035 (2019), *available at* https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3037&context=faculty_scholarship.

[39] Commc'ns Sec., Reliability, and Interoperability Council VI Working Group 3, Final Report on Best Practices and Recommendations to Mitigate Security Risks to Current IP-based Products (Mar. 2019), *available at* https://www.fcc.gov/file/15311/download.

[40] MANRS, *Observatory*, available *at* https://observatory.manrs.org/#/about (last visited Dec. 9, 2019).

Since publication of the road map, initiatives for secure software development have progressed within the public and private sectors. As these projects mature, the challenge will shift to transitioning these tools into widespread use. Agencies have directed federally funded efforts toward botnets, along with complementary efforts to promote successful transition.

Highlights

The 2018 Botnet Report highlighted the importance of secure software development processes and tools to support security throughout the software lifecycle. Significant efforts within the public and private sectors include:

- The National Telecommunications and Information Administration (NTIA) worked to improve software component transparency through a multistakeholder process, with stakeholders publishing a shared vision of a minimum viable software bill of materials (SBOM),[41] a white paper on SBOM standards cross-compatibility,[42] a document offering perspectives on the value of transparency across the ecosystem,[43] and a proof of concept demonstrating the viability and utility of SBOM in the healthcare sector.[44] (Action 1.3)

- NIST released a Draft Cybersecurity White Paper for public comment, Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF).[45] It recommends a core set of high-level secure software development practices that are independent of software development models and programming languages to secure the software development life cycle (SDLC) implementation. These practices are mapped to the industry practices produced by organizations such as SAFECode, BSim, BSA, and the Open Web Application Security Project (OWASP). NIST is currently resolving comments in preparation for the next release of the white paper early in 2020. Upon completion, NIST plans to apply the SSDF taxonomy to the DevOps software development model and IoT devices. (Action 1.3)

- On June 5, 2019, the NSF Office of Advanced Cyberinfrastructure initiated a new cybersecurity innovation research program, "SciTrust: Enhancing Security for Modern Software Programming

[41] Multistakeholder Process on Software Component Transparency Framing Working Grp., Nat'l Telecomms. & Info. Admin., *Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM)* (Nov. 12, 2019), *available at* https://www.ntia.gov/files/ntia/publications/framingsbom_20191112.pdf.
[42] Multistakeholder Process on Software Component Transparency Standards & Formats Working Grp., Nat'l Telecomms. & Info. Admin., *Survey of Existing SBOM Formats and Standards* (Oct. 25, 2019), *available at* https://www.ntia.gov/files/ntia/publications/ntia_sbom_formats_and_standards_whitepaper_-_version_20191025.pdf.
[43] Multistakeholder Process on Software Component Transparency Use Cases & State of Practice Working Grp., Nat'l Telecomms. & Info. Admin., *Roles and Benefits for SBOM Across the Supply Chain* (Nov. 8, 2019), *available at* https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf.
[44] Multistakeholder Process on Software Component Transparency Healthcare Proof of Concept Working Grp., Nat'l Telecomms. & Info. Admin., *Healthcare Proof of Concept Report* (Oct. 1, 2019), *available at* https://www.ntia.gov/files/ntia/publications/ntia_sbom_healthcare_poc_report_2019_1001.pdf.
[45] Donna Dodson et al., *Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)* (June 11, 2019) (Draft), *available at* https://csrc.nist.gov/CSRC/media/Publications/white-paper/2019/06/07/mitigating-risk-of-software-vulnerabilities-with-ssdf/draft/documents/ssdf-for-mitigating-risk-of-software-vulns-draft.pdf.

Cyberinfrastructure," intended to develop artificial intelligence (AI) approaches to the detection of suspicious (non-secure or malicious) software code in open source code repositories online.[46] (Action 1.3)

- In April 2019, BSA: The Software Alliance launched the Framework for Secure Software, a risk-based, outcome-focused tool for describing and assessing security across the software lifecycle.[47] Software development organizations can apply the portions of the framework that are appropriate for their environments and products, based on their own risk analyses and requirements. (Action 1.3)

The 2018 Botnet Report also noted the security benefits of transitioning enterprise networks to Internet Protocol version 6 (IPv6). The NCCoE hosted a workshop on Security for IPv6 Enabled Enterprises in June 2019, and is currently developing a project plan to examine and demonstrate the state of security technologies and guidance specifications for IPv6 enabled enterprises. The NCCoE demonstration project will examine the extent to which current commercially available security technologies can support wide-scale deployment and use of IPv6 in a range of enterprise use case scenarios. (Action 3.4)

While the Botnet Report emphasized deployment of current technologies, it also noted the urgent need to develop new technologies and transition them across the "valley of death"—the gap between federally funded research and a new commercialized technology. Government agencies continue to fund significant research projects and are actively seeking new strategies for technology transition:

- The National Security Agency (NSA) is collaborating with the open source community and private industry to incorporate strong security mechanisms into constrained IoT real time operating systems (RTOS) in the Security Enhancements – Internet of Things (SE – IoT) project. Current collaborations are with the Linux Foundation's Linux and Zephyr Projects and Google's Android and Fuchsia Projects. (Action 1.3)

- From a research perspective, all agencies under the Networking and Information Technology Research and Development (NITRD) Program umbrella include an emphasis on technology transition in the area of network traffic management—for example: NIST's work on MUD, the Extreme DDoS Defense Program (XD3),[48] and the Harnessing Autonomy for Countering Cyber Adversary Systems (HACCS).[49] The NITRD Supplement to the President's Fiscal Year 2019 budget request also included a line item under the Cyber Security and Information Assurance Interagency Working Group's "Detect" research area to fund a joint DHS Science & Technology

---

[46] *CICI: SSC: SciTrust: Enhancing Security for Modern Software Programming Cyberinfrastructure*, Nat'l Sci. Found. (Award Abstract #1839909), *available at* https://www.nsf.gov/awardsearch/showAward?AWD_ID=1839909&HistoricalAwards=false (last visited Dec. 9, 2019).

[47] BSA | The Software Alliance, *The BSA Framework for Secure Software: A New Approach to Securing the Software Lifecycle* (Apr. 2019), *available at* https://www.bsa.org/files/reports/bsa_software_security_framework_web_final.pdf.

[48] Jonathan M. Smith, *Extreme DDoS Defense (XD3)*, Defense Advanced Research Projects Agency, *available at* https://www.darpa.mil/program/extreme-ddos-defense (last visited Dec. 9, 2019).

[49] Dustin Fraze, *Harnessing Autonomy for Countering Cyberadversary Systems (HACCS)*, Defense Advanced Research Projects Agency, *available at* https://www.darpa.mil/program/harnessing-autonomy-for-countering-cyberadversary-systems (last visited Dec. 9, 2019).

Directorate/NIST research project on botnet and malware detection and mitigation.[50] (Action 1.4)

- The National Science Foundation continues to fund technology development work for prevention and mitigation of botnets. The NSF has funded nine awards, totaling nearly $3.5 million, related to botnets since early 2018, such as the SaTC: CORE: Small: Hardening Systems Against Low-Rate DDoS Attacks[51] project and the CRII: OAC: Inferring, Attributing, Mitigating and Analyzing the Malicious Orchestration of Internet-scale Exploited IoT Devices: A Network Telescope Approach[52] project. The NSF's Towards Non-Intrusive Detection of Resilient Mobile Malware and Botnet using Application Traffic Measurement project, awarded in 2016, resulted in several scholarly papers.[53] (Action 1.4)

- The importance of technology transfer was reinforced by the December 2018 publication of the draft NIST Green Paper, Return on Investment Initiative for Unleashing American Innovation.[54] The goal of the Return on Investment Initiative is to maximize the transfer of federal investments in science and technology into value for America in ways that will (a) meet current and future economic and national security needs in a rapidly shifting technology marketplace and enhance U.S. competitiveness globally; and (b) attract greater private sector investment to create innovative products, processes, and services, as well as new businesses and industries. (Action 1.4)

Awareness and Education Line of Effort

This line of effort focuses on building consumer confidence to allow consumers to identify products that meet their needs, adhere to vendors' security claims, and that offer real protection by applying commercially available cybersecurity technologies. It also focuses on educating the existing and emerging workforce on basic cybersecurity.

Public-private efforts to educate consumers and professionals establish a foundation for a more security savvy nation, with marketplace rewards for secure product development and the skills to develop them. Multiple options for accreditation and certification of IoT products have emerged since publication of the road map. As these options mature and market leaders emerge, these processes should contribute to increased consumer confidence and security.

---

[50] Networking & Info. Tech. Research & Dev. Program, *Supplement to the President's FY2019 Budget*, at 16 (Aug. 2018), *available at* https://www.nitrd.gov/pubs/FY2019-NITRD-Supplement.pdf.
[51] *SaTC: CORE: Small: Hardening Systems Against Low-Rate DDoS Attacks*, Nat'l Sci. Found (Award Abstract #1815495), *available at* https://www.nsf.gov/awardsearch/showAward?AWD_ID=1815495 (last visited Dec. 9, 2019).
[52] *CRII: OAC: Inferring, Attributing, Mitigating and Analyzing the Malicious Orchestration of Internet-scale Exploited IoT Devices: A Network Telescope Approach*, Nat'l Sci. Found (Award Abstract #1755179), *available at* https://www.nsf.gov/awardsearch/showAward?AWD_ID=1755179 (last visited Dec. 9, 2019).
[53] *CRII: SaTC: Towards Non-Intrusive Detection of Resilient Mobile Malware and Botnet using Application Traffic Measurement*, Nat'l Sci. Found (Award Abstract #1566388), *available at* https://www.nsf.gov/awardsearch/showAward?AWD_ID=1566388 (last visited Dec. 9, 2019).
[54] Nat'l Inst. of Standards & Tech., *Return on Investment Initiative for Unleashing American Innovation* (Dec. 2018) (NIST Special Publ'n 1234), *available at* https://www.nist.gov/system/files/documents/2018/12/06/roi_initiative_draft_green_paper_nist_sp_1234.pdf.

Highlights

In May 2019, President Trump signed the Executive Order 13870 on America's Cybersecurity Workforce.[55] As directed in EOs 13870 and 13800, and highlighted in the 2018 Botnet Report, the National Initiative for Cybersecurity Education (NICE), led by NIST, continues to promote the NICE Cybersecurity Workforce Framework as a voluntary reference tool for education, training, and workforce development efforts, including as a reference tool for the development of course content, particularly with respect to software development.[56] In particular, NICE held a half-day seminar on November 18, 2019, to help attendees learn how to use and apply the NICE Framework. (Goal 5)

NICE is also addressing early education in cybersecurity to increase awareness, spark interest, and foster skills. The fifth annual NICE K12 Cybersecurity Education Conference was held on December 9-10, 2019, to promote and enrich K12 cybersecurity education programs throughout the country. This year's theme was: "Innovation, Vision, Imagination: Harnessing the talent of today to build the cybersecurity workforce of the future." (Goal 5)

The Global Cyber Alliance worked to educate users around the world, releasing cybersecurity toolkits for small businesses[57] and state and local election officers.[58] The toolkits offer free cybersecurity tools, practical tips, and free resources and guides that will help improve an organization's security posture. As of November 2019, the small business toolkit has been viewed 24,000 times, and the state and local elections officers toolkit 1,300 times. (Goal 5)

DHS continues to analyze the current gaps in the cybersecurity workforce and develop a method to determine the criticality of work roles to better assess and address capability gaps. In 2019, DHS CISA began planning for the Federal Cybersecurity Rotational Program (FCRP), which will aid in the development and growth of the cybersecurity capacity of agencies by providing temporary assignments for federal information technology and cybersecurity employees nominated by their employing agencies. (Action 5.3)

DHS CISA also hosted the first annual President's Cup Cybersecurity Competition—an interagency effort that brought together the government's best personnel supporting cybersecurity and cyber excellence.[59] Competitors faced a diverse array of challenges, incorporated from across the NICE Cybersecurity Framework. The competition consisted of two qualification rounds online, followed by an in-person championship in December 2019. The five finalist teams were given a series of challenges to

---

[55] Exec. Order No. 13870, 84 Fed. Reg. 20,523-20,527 (May 2, 2019), *available at* https://www.federalregister.gov/documents/2019/05/09/2019-09750/americas-cybersecurity-workforce.
[56] National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, NIST Special Publication 800-181 (Aug. 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf; *see also* for up to date versions for the Framework and other activities and resources, NICE Cybersecurity Workforce Framework Resource Center, https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-framework-resource-center (last visited Feb. 14, 2020).
[57] Global Cyber Alliance, *GCA Cybersecurity Toolkit for Small Business*, *available at* https://www.globalcyberalliance.org/gca-cybersecurity-toolkit/ (last visited Dec. 9, 2019).
[58] Global Cyber Alliance, *GCA Cybersecurity Toolkit for Elections*, *available at* https://gcatoolkit.org/elections/ (last visited Dec. 9, 2019).
[59] Cybersecurity & Infrastructure Sec. Agency, U.S. Dep't of Homeland Sec., *Welcome to the 2019 President's Cup Cybersecurity Competition!*, *available at* https://www.cisa.gov/presidentscup (last visited Dec. 9, 2019).

solve on the first day, followed by a virtual escape room on the second day, with the winner determined by a combined score from the two days. (Action 5.3, 5.4)

CISA conducted a series of national webinars to raise stakeholders' awareness of cyber threats and protective actions. CISA hosted eight such webinars in the past year—for example, April 2019's webinar, "Educate and Train Your Cybersecurity Workforce"—reaching more than 6,000 attendees in total. The agency also collaborated with the Small Business Administration and other partners to prepare a strategy and plan for collaborating with the network of Small Business Development Centers across the country to help small businesses increase their cyber resilience. In addition, CISA created and distributed the Cybersecurity Resources Road Map: A Guide for Critical Infrastructure Small and Midsize Businesses, designed to help stakeholders identify and access useful cybersecurity resources based on their needs.[60] (Action 5.5)

In 2019, NIST established the Small Business Cybersecurity Corner[61] to address responsibilities assigned in the NIST Small Business Cybersecurity Act, enacted in August 2018. The act requires NIST to disseminate, and publish on its website, standard and method resources that small business may use voluntarily to help identify, assess, manage, and reduce their cybersecurity risks.[62] These technology neutral, standards-based resources must be sufficiently flexible to apply to small businesses of varying nature and size, independent of the sensitivity of the data collected or stored on the small businesses information systems. (Action 3.2)

The Accreditation Board for Engineering and Technology (ABET), a leading accreditation organization for post-secondary science and engineering education programs, announced that all computing programs accredited by ABET's Computing Accreditation Commission from the 2019-20 accreditation cycle will have to demonstrate that their students are learning cybersecurity appropriate to their discipline.[63] ABET has also begun to encourage inclusion of cybersecurity as a fundamental requirement across engineering disciplines by integrating and piloting new accreditation criteria. Including cybersecurity in engineering disciplines will establish a strong foundation for security in future IoT devices. (Action 5.4)

Another important aspect of this line of effort is the development of accreditation and certification programs to assist consumers (both enterprises and home users) with selecting appropriate products. Commercial programs for device certification against several baselines are now available. CTIA, the wireless industry association, has begun certifying wireless IoT devices under its Internet of Things Cybersecurity Certification Program, announcing that it has certified the first device in March 2019.[64] Underwriter Labs offers a variety of product and safety testing options, as well as testing for many IoT

---

[60] U.S. Dep't of Homeland Sec., *Cybersecurity Resources Road Map: A Guide for Critical Infrastructure, Small and Midsize Business*, *available at* https://www.us-cert.gov/sites/default/files/c3vp/smb/DHS-SMB-Road-Map.pdf.
[61] Nat'l Inst. for Standards & Tech, *Small Business Cybersecurity Corner*, *available at* https://www.nist.gov/itl/smallbusinesscyber (last visited Dec. 9, 2019).
[62] NIST Small Business Cybersecurity Act, Pub. L. No. 115-236, 132 Stat 2444 (2018).
[63] *ABET Approves Accreditation Criteria for Undergraduate Cybersecurity Programs* (Nov. 30, 2018), https://www.abet.org/abet-approves-accreditation-criteria-for-undergraduate-cybersecurity-programs/ (last visited Feb. 18, 2020).
[64] *CTIA IoT Cybersecurity Certification Program Certifies First Device* (March 7, 2019), https://www.ctia.org/news/ctia-iot-cybersecurity-certification-program-certifies-first-device (last visited Feb. 14, 2020).

and wireless standards bodies.[65] Many additional devices have been certified under company and cloud specific programs, such as Microsoft's Azure Certified for IoT program.[66] (Action 5.1)

IV. NSTAC Moonshot Update

Executive Order 13800 called for "resilience against botnets and other automated, distributed threats," directing the Secretary of Commerce, together with the Secretary of Homeland Security, to "lead an open and transparent process to identify and promote action by appropriate stakeholders" with the goal of "dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets)." The Department of Homeland Security's participation was focused through the President's National Security Telecommunications Advisory Committee's (NSTAC) Internet and Communications Resilience subcommittee.

In November 2018, the NSTAC approved and submitted the NSTAC Report to the President on a Cybersecurity Moonshot.[67] The report's primary recommendation was that the government establish a Cybersecurity Moonshot Initiative (Moonshot) to strategically address America's cybersecurity issues. The report stated the Moonshot should focus on six "strategic pillars" to help guide this whole-of-nation effort: 1) technology; 2) human behavior; 3) education; 4) ecosystem; 5) privacy; and 6) policy. The ultimate goal of the Moonshot would be to "make the Internet safe and secure for the functioning of government and critical services for the American people by 2028." The report also recommended that the government establish a series of Cybersecurity Grand Challenges to build momentum by using innovative ideas to achieve immediate improvements to discrete cybersecurity issues.

In response to these recommendations, the National Security Council included the development of Cybersecurity Grand Challenges in its implementation plan for the National Cyber Strategy of the United States of America (2018).[68] Since then, industry convened working groups of key stakeholders to consider current cybersecurity threats, and developed Cybersecurity Grand Challenge topics to address them. Industry also hosted workshops around the report's strategic pillars and how to incentivize stakeholder support around the Moonshot effort.

CISA began researching potential competition topics with a focus on improving the cyber resilience of federal networks and other critical infrastructure sectors.

V. Looking Ahead

In the Botnet Report, published in May 2018, the Departments identified five complementary and mutually supportive goals that, if realized, would dramatically reduce the threat of automated, distributed attacks and improve the resilience and redundancy of the ecosystem:

---

[65] UL Testing, https://www.ul.com/testing (last accessed Feb. 14, 2020).
[66] Microsoft Azure Certified for IoT device catalog, https://catalog.azureiotsolutions.com/learn (last visited Feb. 14, 2020).
[67] Nat'l Sec. Telecomms. Advisory Comm., *NSTAC Report to the President on a Cybersecurity Moonshot* (Nov. 14, 2018), *available at* https://www.cisa.gov/sites/default/files/publications/NSTAC_CyberMoonshotReport_508c.pdf.
[68] Nat'l Sec. Council, *National Cyber Strategy of the United States of America* (Sept. 2018), *available at* https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

- Identify a clear pathway toward an adaptable, sustainable, and secure technology marketplace.
- Promote innovation in the infrastructure for dynamic adaptation to evolving threats.
- Promote innovation at the edge of the network to prevent, detect, and mitigate automated, distributed attacks.
- Promote and support coalitions between the security, infrastructure, and operational technology communities domestically and around the world.
- Increase awareness and education across the ecosystem.

The Botnet Road Map that followed identified discrete steps to achieve these goals, emphasizing that progress must occur across the entire Internet ecosystem. The numerous initiatives detailed in the preceding pages are evidence that we are well on our way, but there is still work to be done. The IoT work, for example, represents an impressive evolution in how government and industry approach IoT security, but it must be sustained over the long term. Across all the lines of effort, the work that is already in progress must continue, and additional activities should build on that work.

In the *IoT Line of Effort*, in November 2019, NIST initiated development of Federal IoT Security Capability baselines with a government-only requirements workshop. This workshop was an important first step toward identifying cybersecurity capabilities required for federal IoT deployment beyond those specified in NISTIR 8259 for incorporation into a federal baseline. The federal baseline is a key milestone on the critical path towards government-wide IoT security policies such as procurement guidelines. Such guidelines would ensure that government investments support and accelerate the development of sustainable markets for secure IoT devices. (Action 1.2)

The private sector also is poised to continue its work, with CSDE, for example, well-positioned to build on its C2 Consensus work to develop operational and policy guidance for shaping, enhancing, and promoting incident response capabilities. A new international standards effort has been initiated in Standards Committee 27 (ISO/IEC JTC1 SC27) to develop internationally accepted security baselines for IoT devices, as discussed above in the *IoT Line of Effort*. That process is expected to take a few years; in the meantime, a draft standard currently known as CTA 2088, which adds specific testable requirements to the capabilities in the C2 Consensus, is expected to be finalized in early 2020. (Action 1.1)

Within the *Enterprise Line of Effort*, new network tools and architectures will enable enterprises to defend their resources from internal and external threats. Advances such as zero trust networking and MUD-aware network management devices will minimize attack surfaces and limit the impact of compromised devices. While driven by IPv4 address exhaustion, transitioning enterprise networks to IPv6 offers additional opportunities for network security. Increased adoption of impactful technologies and practices, such as those published in the CSDE International Anti-Botnet Guide and International Botnet and IoT Security Guide, would also increase security and resilience of the ecosystem. (Actions 1.4, 3.1, 3.3, 3.4)

Within the *Infrastructure Line of Effort*, the momentum established by the MANRS program sets the stage for significant advances in routing security. The MANRS Observatory offers an opportunity to measure and validate these private sector efforts. Changes in ARIN policies, as well as new government-wide policies to support RPKI for federal agency networks, could also contribute to and accelerate these advances by encouraging registration of legacy address blocks and creation of RPKI certificates. (Actions 2.3, 2.5)

Strategies for infrastructure security will need to evolve with the network. In the relatively near future, many devices will be connected solely via 5G, and stakeholders are already working across the ecosystem—in areas like security standards and increased transparency—to improve 5G security in comparison to earlier mobile technologies. One example of planned progress in 5G is the 5G Rural Engagement Initiative, announced by the Competitive Carriers Association (CCA) and the U.S. Chamber of Commerce with sessions that began in October 2019 in Denver, Colorado.[69] This effort will coordinate focused engagement between rural telecom operators and federal agencies closely tied to the issues. The goal is to create a setting that will enable candid discussion and information exchange, and set conditions for persistent engagement, helping to steer the actions of the telecom sector toward a more secure and resilient 5G posture. (Actions 3.3, 3.4)

Within the *Technology Development and Transition Line of Effort*, emerging IoT development platforms that make it easier to meet widely recognized security capability baselines should enhance IoT security with low impact on cost and time to market. As the development platforms incorporating important security capabilities such as secure update, device authentication, and device intent become commonplace, developers will find it much easier to deliver secure products. By amortizing the costs over a large number of developers, the additional costs of a secure software development lifecycle are more easily absorbed. (Actions 1.1, 1.4, 3.2)

In the coming year, stakeholders in NTIA's Software Bill of Materials Multistakeholder Process will continue to refine SBOM practices and extend the working model. Software development stakeholders will look at tooling and processes to make automation easier and cheaper. Others expect to focus on raising awareness and adoption of SBOM practices as key, because the benefits increase as more organizations produce and use SBOM data. Finally, the group will continue demonstrations of the viability and utility of SBOM practices and data in different sectors and use cases. (Actions 1.3, 4.3)

Ongoing research programs, such as the NIST Lightweight Cryptography competition, are expected to contribute additional advances in this line of effort.[70] By establishing a portfolio of proven lightweight cryptographic algorithms, this project will expand the security toolkit for IoT devices that operate on low power. NIST recently selected 32 candidates for Round 2 from the initial set of 56 submissions, and held the Third Lightweight Cryptography Workshop in November 2019. (Actions 1.4, 4.5)

In the *Awareness and Education Line of Effort*, we anticipate advances in professional education and new resources for consumers. Universities and colleges will increasingly incorporate cybersecurity into computer science and engineering curriculums in response to accreditation bodies such as ABET. (Actions 5.3, 5.4)

A key step toward better consumer awareness is an assessment and certification regime that consumers can understand. Widely adopted, efficient, and effective assessment and labeling approaches for IoT devices would allow security-conscious consumers to make informed choices and create market incentives for secure-by-design product development. Some market-specific assessment schemes have

---

[69] *CCA and U.S. Chamber of Commerce Launch 5G Rural Security Engagement Initiative* (Oct. 2, 2019), https://ccamobile.org/press/rca-press-releases/cca-and-u-s-chamber-of-commerce-launch-5g-rural-security-engagement-initiative/9137421 (last visited February 14, 2020).

[70] NIST Lightweight Cryptography Project Overview, https://csrc.nist.gov/projects/lightweight-cryptography (last visited Feb. 14, 2020).

been established, and products are being evaluated against these schemes. This market-based approach will determine optimal methods, including separate assessment regimes for disparate types of devices across the ecosystem. (Action 5.1)

CISA has continued to promote easy-to-adopt, easy-to-understand, and community-endorsed cybersecurity practices, releasing Cyber Essentials guidance in late 2019.[71] Spurred by stakeholders' frequent question of where to start in regard to good cyber hygiene, the Cyber Essentials are designed for small businesses and local governments to understand the basics of cybersecurity. The goal is a whole-of-community approach intended to improve the basic cyber hygiene and resilience of the nation. In parallel, NIST's emerging Small Business Cybersecurity Corner will continue to expand its portfolio of technology neutral, standards-based resources for small businesses. Meanwhile, nonprofit organizations such as the Internet Society and Global Cyber Alliance are continuing to promote their existing initiatives and tools while developing new ones, such as the Global Cyber Alliance's upcoming cybersecurity toolkit for journalists. (Actions 3.2, 4.5, 5.5)

As demonstrated by networking trends, botnets remain a significant threat. Current malicious applications of botnets remain relevant, and attackers continue to devise novel nefarious applications. Without increased deployment of current and emerging technologies to reduce the creation of botnets and mitigate the effects of botnet-driven attacks, the security and resilience of the Internet remains at risk.

The Botnet Report and Botnet Road Map emphasized that neither the U.S. Government, nor any other single entity, can attack the botnet problem alone. The problem of automated, distributed attacks requires action, coordination, and the harnessing of innovation across government and the private sector (including industry, academia, and civil society). This progress update demonstrates a robust effort across the entire ecosystem, and we expect this work to continue. As these efforts mature and customers become aware of the security benefits, increased deployment of these technologies should contribute to the improved security and resilience of the network over time.

[71] Cybersecurity & Infrastructure Sec. Agency, U.S. Dep't of Homeland Sec., *Cyber Essentials* (Nov. 6, 2019), *available at* https://www.cisa.gov/sites/default/files/publications/19_1106_cisa_CISA_Cyber_Essentials_S508C.pdf.