A Road Map
Toward Resilience Against Botnets

November 29, 2018

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 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. This initial road map lays 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] The road map identifies five lines of effort, each with a set of tasks and timelines for completion. In this initial version, 85 tasks are listed, but that number will change over time as some tasks are completed and new tasks arise.

As explained in the Botnet Report, many of the report's actions are mutually supportive by design, even across goals. Some actions are already in progress, others are dependent on outside factors, and a final set awaits leadership and/or funding. We do not expect all actions to occur simultaneously, due to considerations such as resource constraints or varying levels of sophistication in the relevant stakeholder communities. It is also worth noting that, while these actions were identified in the Botnet Report, implementing the actions will make the overall Internet ecosystem more secure and have an impact far beyond the boundaries of the report itself.

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

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

Some tasks will be the direct responsibility of the federal government, while others are specific to the private sector. Some tasks do not directly involve the federal government, but support, or are supported by, actions that depend on federal involvement or leadership. By indicating its own priorities, the federal government can increase stakeholder confidence that resources invested in industry-led actions with federal dependencies will result in productive outcomes.

---

[1] Exec. Order No. 13,800, 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/page/report-president-enhancing-resilience-against-botnets.
[4] Nat'l Sec. Council, National Cyber Strategy of the United States of America (September 2018), *available at* https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

The Departments of Commerce and Homeland Security continue to welcome interest from members of the private sector who wish to contribute to an action in the Botnet Report. Many of the road map actions should be led by industry, academia, or civil society. Where applicable, this road map identifies existing private-sector leaders or governance structures for the relevant tasks. Where existing bodies are already pursuing related actions, or already represent key communities, they are encouraged to lead. Government has the power to convene and will do so, but achieving the outcomes set forth in the Botnet Report will require industry and civil society engagement from across the ecosystem. The identified tasks and associated information should be seen as non-binding and flexible to accommodate changes in the digital ecosystem over time.

In cases where a mutually agreed party or parties from the private sector has not yet been identified to lead, the federal government will provide a coordination and communication mechanism. The federal government will also meet periodically with the relevant parties to facilitate collaboration and share findings. Those organizations identified as "contributors" in the task breakouts below make up a non-exhaustive list of current efforts that are contributing toward solutions. Organizations are encouraged to look for opportunities to collaborate and partner to the extent feasible. The U.S. government values innovation, and expects the market to determine the most expeditious solutions to the identified concerns.

In addition to federal dependencies, some actions have a natural temporal ordering. For example, the assessment programs in Actions 5.1 and 5.2 depend upon the establishment of appropriate security capability baselines in Action 1.1, and therefore cannot begin immediately. Other actions are ripe for prioritization because the work is already underway, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) profile described in Action 2.2. Finally, some actions have special urgency because of long lead-time (e.g., Actions 1.3, 5.3, and 5.4) or because developments are narrowing the window for the United States to influence the direction (Action 1.2).

Finally, to track progress, the Department of Commerce (Commerce) and the Department of Homeland Security (DHS) will develop a 365-day status update for the President, due one year after the road map's initial publication. This update will review: 1) progress the community as a whole is making against the road map; 2) the impacts of those road map activities; 3) a reassessment of the threat of automated, distributed attacks, including whether the threat is increasing or decreasing, and any known reasons for such a change; and 4) what activities should be prioritized in the coming year.

II. Road Map

The following subsections present tasks drawn from the 24 actions laid out in the Botnet Report in the context of five *lines of effort*:

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

The five lines of effort are themselves subdivided into *workstreams* composed of *tasks*. Where tasks have dependencies, the tasks are furthered organized into a *series*. Each task description includes a

brief summary and a reference to a Botnet Report action number, identifies task leaders (if determined) and supporting players, identifies tasks that must be completed before starting or completing, and proposes start and completion dates by calendar year quarter**.** Commerce and DHS welcome feedback from stakeholders on all elements of the road map tasks, particularly identification of leads and contributing partners for identified actions, as well as timelines.

IoT Line of Effort: Raising the Bar for IoT Security

The Botnet Report recognized the impact of connected devices on the ability to extend the scope and scale of automated, distributed attacks against ecosystem targets. The Internet of Things (IoT) Line of Effort focuses on reducing security risk across the IoT ecosystem through the establishment of baseline security standards applied across the full lifecycle of connected devices.

IoT Workstream 1: Developing Robust Markets for Trustworthy IoT Devices

This workstream focuses on the development of a robust market for devices that offer appropriate security capabilities for three sectors: consumers/home users, industrial users, and the federal government. The foundational initial task describes a core set of security capabilities that are broadly applicable (ideally, applicable to all three sectors) and can be supported by a broad range of assessment schemes. Once the core has been defined, concurrent series of tasks are launched for each of the three sectors. Each series of tasks defines a superset of the core baseline suitable for that sector, followed by a set of supporting activities designed to develop a robust market for conforming products.

Defining a Core Security Capability Baseline

This task establishes a core set of security capabilities required for secure deployment of IoT devices, regardless of the intended environment. Core security capabilities should be provided or facilitated by common development platforms to limit impact on time to market and enable innovation. These baseline capabilities must also be appropriate for both attestation-based and third-party evaluation-based conformity assessment schemes.

> *Task Name: Define Core Security Capability Baseline*
> Action Number: 1.1
> Task Summary: Compare/analyze different baseline documents to Identify widely accepted and broadly applicable "core security capabilities" that could be supported by the full range of assessment schemes. At a minimum, the capability baseline would address device and data security. NIST will publish the consensus baseline as a NIST white paper or Interagency Report (NISTIR) for reference and use in future tasks.
> Contributor(s): NIST (Lead), baseline owners, developer kit vendors, consumer consortia, Council to Secure the Digital Economy (CSDE)[5]/Consumer Technology Association (CTA)
> Prerequisite Tasks: N/A
> Anticipated Start[6]: 1Q19
> Expected Completion: 3Q19

[5] *See* Council to Secure the Dig. Econ., *available at* https://securingdigitaleconomy.org/
[6] All start dates are calendar year estimates and subject to resource determinations.

Establish a Robust Market for Trustworthy Consumer/Home IoT Devices

The following tasks are designed to establish a widely adopted security capability baseline for consumer/home IoT products with high product availability and strong customer recognition. These tasks begin by augmenting the core security capability baseline with requirements specific to the consumer/home IoT market. To encourage development and deployment of conforming devices, an attestation or assessment scheme is created along with educational and awareness tools that will help customers make informed choices about IoT purchases.

Task Name: Develop Consumer/Home IoT Security Baseline
Action Number: 1.1
Task Summary: Build on core capabilities to identify security baseline appropriate for consumer/home IoT.
Contributor(s): IoT industry, civil society, NIST, CSDE/CTA
Prerequisite Tasks: Publish core security capability baseline
Anticipated Start: 2Q19
Expected Completion: 1Q20

Task Name: Establish or Support Assessment Programs for Consumer/Home IoT Devices
Action Number: 5.1
Task Summary: Establish or support agile assessment or attestation programs for consumer/home IoT devices that meet the above baseline.
Contributor(s): Industry, civil society, CTIA, NIST, other U.S. government (USG) stakeholders, CSDE/CTA
Prerequisite Tasks: Develop consumer/home IoT security baseline
Anticipated Start: In progress
Expected Completion: 2Q20

Task Name: Explore Labeling for Consumer/Home IoT
Action Number: 5.1
Task Summary: Explore utility of a voluntary labeling approach, or other informational options, to improve consumer/home IoT device consumer awareness.
Contributor(s): Federal Trade Commission (FTC), NTIA, other federal partners, IoT industry, retailers, civil society, academia, CSDE/CTA
Prerequisite Tasks: N/A
Anticipated Start: 4Q19
Expected Completion: 4Q20

Task Name: Implement Awareness Strategies for Trustworthy Consumer/Home IoT Devices
Action Number: 5.1
Task Summary: Develop informational tools such as labeling or branding that assist motivated consumers in identification of conforming consumer/home IoT products.
Contributor(s): IoT industry, retailers, CSDE/CTA
Prerequisite Tasks: Establish assessment program for consumer/home IoT devices; explore labeling for consumer/home IoT
Anticipated Start: 2Q20
Expected Completion: 2Q21

Task Name: Federal Support for Consumer/Home IoT Security Baseline & Assessment

Action Number: 5.5
Task Summary: Increase USG engagement with targeted user communities and civil society to promote awareness and acceptance of the consumer/home IoT security baseline and supporting assessment program(s); leverage DHS' existing awareness activities, such as STOP.THINK.CONNECT.
Contributor(s): DHS, Commerce, FTC, civil society
Prerequisite Tasks: Develop consumer/home IoT security baseline; establish assessment program for home IoT devices.
Anticipated Start: 2Q20
Expected Completion: 1Q23

Establish a Robust Market for Trustworthy Industrial IoT Devices

The following tasks are designed to establish a widely adopted security capability baseline for Industrial IoT products with high product availability and strong customer recognition. These tasks begin by augmenting the core security capability baseline with requirements specific to the Industrial IoT market. To encourage development and deployment of conforming devices, one or more assessment schemes are created along with educational and awareness tools to inform customers.

Task Name: Develop Industrial IoT Security Baseline
Action Number: 1.1
Task Summary: Build on core capabilities to identify security baseline appropriate for industrial/SCADA environments.
Contributor(s): Industrial IoT industry, national labs, DHS, sector-specific agencies, sector coordinating councils (e.g., Energy, Health, Transportation)
Prerequisite Tasks: Publish core security capability baseline
Anticipated Start: 2Q19
Expected Completion: 4Q19

Task Name: Establish Assessment Program for Industrial IoT Devices
Action Number: 5.2
Task Summary: Establish cost effective assessment program(s) for industrial IoT devices that meet the baseline requirements.
Contributor(s): Industrial IoT industry, national labs, DHS, sector-specific agencies, sector coordinating councils (e.g., Energy, Health, Transportation)
Prerequisite Tasks: Develop industrial IoT security baseline
Anticipated Start: 4Q19
Expected Completion: 2Q20

Task Name: Explore Labeling or Other Transparency Scheme for Industrial IoT Devices
Action Number: 5.2
Task Summary: Work to develop a voluntary labeling approach, or other information transparency schema, as an option for informing industrial enterprise customers.
Contributor(s): Industrial IoT industry, national labs, DHS, sector-specific agencies, sector coordinating councils (e.g., Energy, Health, Transportation)
Prerequisite Tasks: Develop industrial IoT security baseline
Anticipated Start: 4Q19
Expected Completion: 4Q20

Task Name: Support Awareness for Customers of Industrial IoT Devices
Action Number: 5.2
Task Summary: Create informational tools such as labels or branding that help industrial enterprise customers identify conforming industrial IoT products.
Contributor(s): Industrial IoT industry, retailers, DHS through the National Council of Information Sharing and Analysis Centers (ISACs)
Prerequisite Tasks: Develop industrial IoT security baseline
Anticipated Start: 2Q20
Expected Completion: 4Q20

Task Name: Promote Adoption of Assessment Regime by Critical Infrastructure
Action Number: 5.2
Task Summary: Through the ISAC Council, DHS and industry will evaluate commercial certification regime(s) for IoT and IT products as they emerge for applicability to critical infrastructure.
Contributor(s): DHS (Lead), industrial IoT industry, national labs, DHS, sector-specific agencies, sector coordinating councils (e.g., Energy, Health, Transportation)
Prerequisite Tasks: Establish assessment program for industrial IoT devices
Anticipated Start: 3Q20
Expected Completion: 2Q21

Establish a Robust Market for Trustworthy Federal IoT devices

The following tasks are designed to establish a widely adopted security capability baseline for federal IoT products with high product availability and strong customer recognition. These tasks begin by augmenting the core security capability baseline with requirements specific to the federal IoT market. To encourage acquisition and deployment of conforming devices, federal procurement regulations are established that reference the federal baseline.

Task Name: Identify Federal IoT Security Requirements
Action Number: 2.3
Task Summary: Convene key stakeholders in a series of meetings to identify non-core security capabilities that are common/specific to federal environments.
Contributor(s): Office of Management and Budget (OMB), General Services Administration (GSA), Department of Defense (DOD), DHS, NIST, Federal Chief Information Officer (CIO) Council, federal chief information security officers (CISOs)
Prerequisite Tasks: Publish core security capability baseline
Anticipated Start: TBD
Expected Completion: TBD

Task Name: Specify Federal IoT Security Capability Baseline
Action Number: 2.3
Task Summary: In collaboration with industry and agencies, develop and publish a federal IoT security capability baseline.
Contributor(s): NIST (Lead), DHS, Federal CIO Council, federal CISOs, industry, CSDE/CTA
Prerequisite Tasks: Identify federal IoT security requirements
Anticipated Start: 3Q19
Expected Completion: 1Q20

Task Name: Establish Federal IoT Procurement Regulations
Action Number: 2.3
Task Summary: Establish federal procurement regulations to support acquisition of IoT devices consistent with the federal IoT security capability baseline.
Contributor(s): GSA (Lead), OMB, Federal CIO Council, federal CISOs, and procurement officers
Prerequisite Tasks: Specify federal IoT security capability baseline
Anticipated Start: TBD
Expected Completion: TBD

IoT Workstream 2: Adoption and Sustainability for IoT Security

This workstream focuses on the development of the global ecosystem for IoT devices in general. That is, the portfolio of actions specified in this workstream 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.

Extending Risk Management for IoT

Many enterprise cybersecurity programs have shifted to risk-based approaches, such as NIST's Cybersecurity Framework. The standards, guidelines, and best practices these organizations leverage to manage cybersecurity-related risk using the Framework and related approaches have historically focused on information technology (IT) and traditional IT networks. In this series of tasks, risk management approaches are extended to help organizations better understand and manage the cybersecurity and privacy risks associated with their IoT devices throughout their lifecycles.

Task Name: Enable Risk Management Approach to IoT Security
Action Number: 1.5
Task Summary: Publish NISTIR 8228, "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks," to support risk management approaches to IoT security.
Contributor(s): NIST (Lead), industry
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: 1Q19

Task Name: Publish Best Practices for IoT Device Manufacturers
Action Number: 1.5
Task Summary: Identify best practices that contribute to customer outcomes identified in the emerging NISTIR 8228, "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks" using the core security capabilities.
Contributor(s): NIST (Lead), TBD
Prerequisite Tasks: Enable risk management approach to IoT security; publish core security capability baseline
Anticipated Start: 2Q19
Expected Completion: 2Q20

Task Name: Commoditize Secure Update Technologies

Action Number: 1.5
Task Summary: Promote standards and commercial frameworks for secure updates. Encourage IoT developer kits to incorporate secure update mechanisms to minimize developers' time to market. Publish Internet Engineering Task Force (IETF) specifications for Secure Update for IoT devices to encourage off-the-shelf support for security patches.
Contributor(s): IETF participants, NIST, NTIA, other
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: 2Q19

Task Name: Align Usability and Manageability with Customer Abilities
Action Number: 3.2
Task Summary: Prioritize simple and straightforward deployment and configuration processes for devices marketed to home and small businesses.
Contributor(s): Consumer Technology Association (CTA), IT and IoT industry
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: Ongoing

Establish Globally Relevant IoT Standards

The Botnet Report noted that "U.S. government and industry should jointly engage with developers of industry-led, voluntary international standards and specifications to establish globally relevant standards." This series of tasks encourages U.S. government and industry to jointly pursue international standards consistent with the capability baselines developed in the previous workstream.

Task Name: Establish Globally Relevant IoT Standards
Action Number: 1.2
Task Summary: The U.S. government and industry should, through inclusive discussion processes, jointly identify a key set of venues for development of voluntary international IoT security standards and initiate standards activity. Participants can introduce the core security capability baseline as a contribution once the baseline is completed.
Contributor(s): NIST, NTIA, DHS, IICSWG, IoT industry
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: 4Q19

Task Name: Identify Incentives for IoT Adoption of Security Standards
Action Number: 2.3
Task Summary: Identify existing and needed incentives for private sector adoption of IoT security standards and baselines, which can be adopted by the USG.
Contributor(s): IoT industry, DHS, Commerce, FTC, sector-specific agencies, sector coordinating councils
Prerequisite Tasks: Establish globally relevant IoT standards
Anticipated Start: TBD
Expected Completion: TBD

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 automated, distributed attacks.

The Enterprise Line of Effort has four complementary workstreams:

- CSF profiles for mitigation and protection
- Migration to advanced enterprise network architectures
- Federal adoption of enterprise best practices
- Operational technology

Enterprise Workstream 1: CSF Profiles for Mitigation and Protection

The NIST Cybersecurity Framework has become an essential tool for enterprises and agencies that employ a risk-based approach to achieving appropriate security outcomes. This series of tasks establishes industry consensus CSF profiles for mitigating distributed denial of service (DDoS) threats and combatting botnets. After completion of the industry-led profiles, the federal government tailors these profiles for the federal environment.

Task Name: Develop CSF Profile for DDoS Mitigation
Action Number: 2.2
Task Summary: Work with industry to develop consensus CSF Profile for DDoS Mitigation.
Contributor(s): Cybersecurity Coalition (Lead),[7] digital ecosystem industry, NIST, NTIA, DHS, civil society
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: 1Q19

Task Name: Publish Federal CSF Profile for DDoS Mitigation
Action Number: 2.3
Task Summary: Publish Federal CSF Profile for DDoS Mitigation as a NIST Special Publication.
Contributor(s): NIST (Lead), DHS, federal agencies, digital ecosystem stakeholders, civil society
Prerequisite Tasks: Develop CSF Profile for DDoS Mitigation
Anticipated Start: 2Q19
Expected Completion: 3Q19

Task Name: Develop CSF Profile for Botnet Threat Mitigation
Action Number: 2.2
Task Summary: Develop industry consensus CSF Profiles for Botnet Threat Mitigation.
Contributor(s): Cybersecurity Coalition (Lead), digital ecosystem stakeholders, NIST, NTIA, DHS, civil society
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: 2Q19

[7] *See* Cybersecurity Coalition, *available at* https://www.cybersecuritycoalition.org/

Task Name: Publish Federal CSF Profile for Botnet Threat Mitigation
Action Number: 2.3
Task Summary: Publish Federal CSF Profile for Botnet Threat Mitigation as a NIST Special Publication.
Contributor(s): NIST (Lead), DHS, federal agencies, digital ecosystem stakeholders, civil society
Prerequisite Tasks: Develop CSF Profile for Botnet Threat Mitigation
Anticipated Start: 2Q19
Expected Completion: 3Q19

Task Name: Raise Enterprise Awareness for DDoS Mitigation
Action Number: 3.3
Task Summary: Establish partnership campaigns and strategic engagement activities to improve user and enterprise knowledge of automated distributed threats and best security practices.
Contributor(s): Cybersecurity Coalition, NTIA, DHS, NIST, civil society
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: TBD

Enterprise Workstream 2: Advancing Enterprise Network Architectures

Enterprises should migrate to network architectures that facilitate detection, disruption, and mitigation of automated, distributed threats. They should also consider how their own networks put others at risk. In this workstream, a series of concurrent activities identify current best practices and explore emerging technologies for enterprise network architectures.

Task Name: Enhance and Evolve Best Practices on Enterprise Network Traffic Management
Action Number: 3.1
Task Summary: Enhance and evolve constructive policies and best practices on enterprise network traffic management across targeted ecosystem sectors, keeping in mind the requirements of small businesses. Evolve best practices as technologies and architectures advance, and address gaps in best practices for new players and entrants.
Contributor(s): CSDE /CTA (Lead), industry coordination groups, enterprise network operators, network operator groups (NOGs), network engineers, NIST, NTIA, DHS, DOD, Internet service providers, infrastructure providers, global digital ecosystem enterprises, civil society
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: 2Q2019

Task Name: Promote Enterprise Network Architectures that Mitigate Risks of Automated, Distributed Threats
Action Number: 3.3
Task Summary: Promote the implementation and adoption of advanced enterprise network architectures that mitigate risk of automated, distributed threats. Identify where gaps in enterprise adoption proliferate, and undertake efforts to understand market and policy barriers to integration and deployment.
Contributor(s): CSDE, industry coordination bodies, enterprise network engineers and operators, NOGs, NTIA, NIST, DHS, Committee on National Security Systems (CNSS), academia, civil society

Prerequisite Tasks: Enhance and evolve best practices on network traffic management
Anticipated Start: 2Q2019
Expected Completion: TBD

Task Name: Accelerate Domestic Availability of IPv6 Internet Services
Action Number: 3.4
Task Summary: Government works with stakeholders to support full transition to IPv6 by Internet service providers (ISPs) by identifying lessons learned from industry and other countries, identifying both impediments to transition and potential incentives.
Contributor(s): NTIA (Lead), Regional Internet Registries (RIRs), ISPs, IT and IoT industry
Prerequisite Tasks: N/A
Anticipated Start: 4Q19
Expected Completion: 2Q20

Task Name: Accelerate Transition to IPv6 Enterprise Networks
Action Number: 3.4
Task Summary: Demonstrate the impact and practicality of IPv6-only enterprise IT deployment.
Contributor(s): NIST (Lead), industry
Prerequisite Tasks: N/A
Anticipated Start: TBD
Expected Completion: TBD

Task Name: Establish Requirements for Zero Trust Networking (ZTN)
Action Number: 3.3
Task Summary: Federal CIO Council Zero Trust Networking Working Group will develop initial requirements for agency deployment of zero trust networking (ZTN). Using these requirements, departments and agencies will be positioned to incorporate these features as responsive technologies emerge.
Contributor(s): Federal CIO Council Zero Trust Networking Working Group (Lead)[8]
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: 4Q18

Task Name: Evaluate Current Feasibility of ZTN
Action Number: 3.3
Task Summary: National Cybersecurity Center of Excellence (NCCoE) and industry collaborators will perform a feasibility study for ZTN requirements identified by the CIO Council's ZTN Working Group using commercial and emerging technologies.
Contributor(s): NIST (Lead), DHS, CIO Council Zero Trust Networking Working Group
Prerequisite Tasks: Establish requirements for zero trust networking
Anticipated Start: In progress
Expected Completion: 4Q19

Task Name: Identify Best Practices for IoT Network Management
Action Number: 1.5

[8] *See* About the Council, CIO Council, *available at* https://www.cio.gov/about/.

Task Summary: Using the results of the NCCoE Mitigating IoT-Based DDoS project and ZTN feasibility study, NIST will identify current best practices for enterprise network management where environments include IoT devices.
Contributor(s): NIST (Lead), DHS, digital ecosystem industry and civil society stakeholders
Prerequisite Tasks: Evaluate current feasibility of ZTN; mitigating IoT-based DDoS
Anticipated Start: 3Q19
Expected Completion: 2Q20

Enterprise Workstream 3: Federal Adoption of Enterprise Best Practices

Stakeholders indicated that federal adoption of "good neighbor" practices would provide an ecosystem-wide foundation for further activities to reduce automated, distributed threats. In particular, steps by federal agencies to implement egress filtering to prevent network address spoofing, close reflectors used to amplify traffic volumes, and measure agency compliance (and potentially name and shame bad actors) would demonstrate federal resolve and encourage beneficial action by other parties. In this series of tasks, the federal government performs activities to ensure that these best practices are properly reflected in federal agency policies, standards, guidelines, and oversight.

Task Name: Federal Adoption of Federal CSF Profiles for Automated, Distributed Threats
Action Number: 2.3
Task Summary: OMB issues guidance to agencies, including timelines for adoption and reporting, regarding adoption of federal CSF profiles for automated distributed threats. NIST creates or identifies measurement tools to quantify progress.
Contributor(s): OMB e-Gov (Lead), NIST, DHS, other USG agencies
Prerequisite Tasks: Federal CSF Profile for DDoS Mitigation; Federal CSF Profile for Botnet Prevention and Mitigation
Anticipated Start: In progress
Expected Completion: 2Q20

Task Name: Implement Ingress/Egress Filtering in All U.S. Federal Agency Networks
Action Number: 2.3
Task Summary: Federal agencies ensure that agency networks and commercially provisioned network information services take active measures to prevent traffic with spoofed network source addresses.
Contributor(s): DHS (Lead), GSA, OMB, other federal agencies, federally contracted service providers
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: 3Q19

Task Name: Develop Federal Security Guidelines for Reflectors
Action Number: 2.3
Task Summary: Supplement existing NIST guidelines for operating DNS servers and resolvers with a NIST Special Publication establishing general guidelines for operation of Network Time Protocol (NTP) and other User Datagram Protocol (UDP)-based widely deployed resources.
Contributor(s): NIST (Lead), DHS
Prerequisite Tasks: N/A
Anticipated Start: In progress

Expected Completion: 2Q19

Task Name: Implement Federal Security Guidelines for Reflectors
Action Number: 2.3
Task Summary: Mandate implementation of NIST guidelines for reflective resources by all federal agencies.
Contributor(s): DHS (Co-Lead), OMB (Co-Lead), NIST
Prerequisite Tasks: Develop federal security guidelines for reflectors
Anticipated Start: 2Q19
Expected Completion: 2Q20

Task Name: Track and Remediate Vulnerable Resources at Federal Agencies
Action Number: 2.3
Task Summary: Develop list of federal agencies with reflective resources that are out-of-compliance with NIST guidelines and track progress.
Contributor(s): DHS (lead), OMB, U.S. departments and agencies
Prerequisite Tasks: Adoption of federal CSF profiles for automated, distributed threats
Anticipated Start: 2Q20
Expected Completion: Ongoing

Enterprise Workstream 4: Operational Technology

A series of tasks are specified below that seek to close gaps in understanding between the cybersecurity and operational technology (OT) communities. Cybersecurity experts often have limited awareness of limitations and constraints imposed by OT-specific concerns (e.g., safety), while the operational technology community has limited awareness of cybersecurity risks and capabilities.

Task Name: Cybersecurity and OT Communities Collaborate to Improve Understanding of OT Cybersecurity Challenges
Action Number: 4.5
Task Summary: Cybersecurity community works with OT community to improve understanding of cybersecurity challenges.
Contributor(s): DHS (Lead), sector-specific agencies, national labs, sector coordinating councils
Prerequisite Tasks: N/A
Anticipated Start: 2Q19
Expected Completion: 3Q21

Task Name: Expand OT-Cybersecurity Information Sharing
Action Number: 4.5
Task Summary: Expand current federal engagements that promote information sharing between OT and cybersecurity communities.
Contributor(s): DHS (Lead), sector-specific agencies, national labs, sector coordinating councils
Prerequisite Tasks: N/A
Anticipated Start: 2Q19
Expected Completion: 3Q21

Task Name: Promote OT Adoption of IT Security Technology
Action Number: 4.5

Task Summary: Expand current federal engagements that promote OT adoption of IT security technology.
Contributor(s): NIST (Lead), DHS, sector-specific agencies, sector coordinating councils
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: 3Q21

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.

The Infrastructure Line of Effort has four complementary workstreams:

- Improvements to routing security
- Information sharing in practice
- Information sharing protocols
- Research and development

Infrastructure Workstream 1: Improvements to Routing Security

The Internet was designed to facilitate resilient communications between end points, and provided less regard to basic security services. As a result, the state of routing security on the Internet falls far below what can be achieved with both common and newer tools and practices. This series of tasks advances deployment of longstanding anti-spoofing technologies and newer technologies to protect against route hijacks and leaks.

Task Name: Remove Legal and Policy Barriers to Resource Public Key Infrastructure (RPKI) Adoption
Action Number: 2.3
Task Summary: Establish consensus legal strategy to address barriers to RPKI adoption, including RPKI certificate issuance for legacy address holders, liability issues, and barriers to alternative deployment models.
Contributor(s): Academia, Internet engineers, NIST, NTIA, DOD, regional and local Internet registries
Prerequisite Tasks: N/A
Anticipated Start: 2Q19
Expected Completion: 1Q20

Task Name: Federal Agencies Adopt RPKI
Action Number: 2.3
Task Summary: Federal address holders and service providers create route origin authorizations (ROAs) for address resources and apply ROAs to Internet routing decisions to mitigate route hijacks.
Contributor(s): DHS (Lead), OMB, DOD, federal agencies
Prerequisite Tasks: Remove legal and policy barriers to RPKI adoption
Anticipated Start: 1Q20
Expected Completion: 1Q21

Task Name: Increase Scalability and Robustness of Anti-Spoofing Mechanisms
Action Number: 2.3
Task Summary: Government and industry continue research to make anti-spoofing more scalable and robust, and available at all levels of the Internet.
Contributor(s): DHS (Lead), federal technology incubators, NIST, Internet engineers, academia
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: 4Q19

Task Name: Extend Adoption, Awareness and Application of Anti-Spoofing Mechanisms
Action Number: 2.3
Task Summary: Promote adoption and extend the implementation of anti-spoofing mechanisms, as appropriate, throughout the Internet infrastructure.
Contributor(s): Internet infrastructure owners and operators, civil society, NIST, NTIA, DHS
Prerequisite Tasks: Increase scalability and robustness of anti-spoofing mechanisms
Anticipated Start: 4Q19
Expected Completion: 4Q20

Task Name: Establish Mutually Agreed Norms for Routing Security (MANRS) Observatory and Dashboard for Routing Security Metrics
Action Number: 2.5
Task Summary: Develop metrics and website to assess the security and resilience of the Internet routing system over time.
Contributor(s): Internet Society, RIRs
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: 4Q18

Task Name: Develop Security Requirements for Internet Services
Action Number: 3.3
Task Summary: Publish SP 800-189, "Secure Inter-Domain Traffic Exchange: BGP Robustness and DDoS Mitigation."
Contributor(s): NIST (Lead)
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: 2Q19

Task Name: Explore Evolution of Threats and Emerging Solutions Around Routing Security
Action Number: 3.3
Task Summary: Engage stakeholders and Internet infrastructure actors to understand the benefits and limits of existing and emerging routing security solutions, capturing stakeholder concerns and potential mitigations.
Contributor(s): NTIA, Internet infrastructure owners and operators, civil society, NIST, DHS
Prerequisite Tasks: N/A
Anticipated Start: 3Q19
Expected Completion: 3Q20

Infrastructure Workstream 2: Information Sharing in Practice

Large network providers currently share network management techniques and defensive tactics that are effective against particular threats. Law enforcement depends upon information from the private sector to initiate investigations. This series of tasks focuses on extending information sharing to smaller ISPs and foreign network providers, and ensuring that law enforcement is alerted at the earliest possible stage, while respecting privacy guidelines and regulations.

Task Name: Increase Smaller ISPs' Access to Industry-Shared Threat Information
Action Number: 2.1
Task Summary: Expand domestic information sharing to enhance participation of smaller ISPs.
Contributor(s): Infrastructure providers, DHS through the Communications ISAC
Prerequisite Tasks: N/A
Anticipated Start: TBD
Expected Completion: TBD

Task Name: Expand Global and Regional Threat Information Sharing
Action Number: 2.1
Task Summary: Enhance information sharing mechanisms to facilitate expanded global and regional sharing.
Contributor(s): Global computer security incident response teams (CSIRTs), DHS, NOGs, ISACs, infrastructure providers
Prerequisite Tasks: N/A
Anticipated Start: 1Q19
Expected Completion: TBD

Task Name: Expand Information Sharing Agreements
Action Number: 2.1
Task Summary: U.S. government leverages ISACs, NOG partnerships, Forum of Incident Response and Security Teams (FIRST), and works with international peers to expand information-sharing agreements.
Contributor(s): DHS, NOGs, ISAC Council, ISACs, FIRST, law enforcement partnerships, cyber center/fusion centers
Prerequisite Tasks: N/A
Anticipated Start: TBD
Expected Completion: TBD

Task Name: Share Timely and Actionable Information with Law Enforcement
Action Number: 4.1
Task Summary: Provide even more timely and actionable information to facilitate, support, and accelerate law enforcement actions, including those that affect botnets distributed across the globe.
Contributor(s): Department of Justice (DOJ)/Federal Bureau of Investigations (FBI), FTC, ISACs, DHS, NOGs, global CSIRTs, large enterprises and infrastructure providers
Prerequisite Tasks: N/A
Anticipated Start: TBD
Expected Completion: TBD

Task Name: Improve U.S. Government Information Sharing with Industry
Action Number: 4.1
Task Summary: Improve timeliness and relevance of information shared by U.S. government with industry.
Contributor(s): USG Cyber Centers, DHS, Sector-Specific Agencies, ISAC/information sharing and analysis organizations (ISAOs)
Prerequisite Tasks: N/A
Anticipated Start: TBD
Expected Completion: TBD

Task Name: Enhance Accuracy of Security-Critical Data Resources
Action Number: 4.1
Task Summary: WHOIS databases, comprised of registration information for Internet naming and numbering resources (e.g., IP addresses and domain names), are improved for accuracy to facilitate attribution of bad actors. Mechanisms are developed that preserve timely access to WHOIS information while satisfying privacy protection regulations (e.g., EU General Data Protection Regulation [GPDR]) and supporting botnet investigatory work.
Contributor(s): Domain name registries/registrars, NTIA, the Internet Corporation for Assigned Names and Numbers (ICANN), RIRs, Law Enforcement, academia, and civil society
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: Ongoing

Infrastructure Workstream 3: Information Sharing Protocols

This collection of tasks focuses on standardization of information-sharing protocols to increase speed and permit automated response. Enhancing the utility of information sharing protocols complements the information-sharing process tasks by increasing the value of the information that is shared.

Task Name: Support Information Sharing Automation
Action Number: 2.1
Task Summary: Enhance information-sharing protocols to increase speed and support automated response.
Contributor(s): DHS, ISAOs, industry, civil society, consortia
Prerequisite Tasks: N/A
Anticipated Start: TBD
Expected Completion: TBD

Task Name: Support Collaborative Incident Response
Action Item: 4.4
Task Summary: IETF finalizes the DDoS Open Threat Signaling (DOTS) protocol. Enterprises with multi-party DDoS mitigation strategies implement and deploy DOTS to facilitate coordinated action.
Contributor(s): IETF, digital ecosystem enterprises, civil society
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: TBD

Task Name: Enhance Information-Sharing Protocols to Facilitate Global Information Sharing
Action Number: 2.4
Task Summary: The U.S. government and industry will review and enhance information-sharing protocols, such as Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII), to facilitate global information sharing with respect to automated threats.
Contributor(s): DHS (Lead), ISAOs, federally funded research and development centers (FFRDCs), industry
Prerequisite Tasks: N/A
Anticipated Start: TBD
Expected Completion: TBD

Task Name: Establish International Standards to Facilitate Information Sharing
Action Number: 2.4
Task Summary: Industry, with support from the U.S. government, will establish international standards for information sharing to facilitate global coordination.
Contributor(s): Industry (lead), DHS, ISAC/ISAOs, civil society
Prerequisite Tasks: N/A
Anticipated Start: TBD
Expected Completion: TBD

Infrastructure Workstream 4: Research and Development

Task Name: Incorporate Infrastructure Best Practices into the NIST Cybersecurity Framework
Action Number: 3.3
Task Summary: Continually evaluate advances in best security practices and technology for inclusion in the NIST Cybersecurity Framework.
Contributor(s): NIST (lead), infrastructure providers
Prerequisite Tasks: N/A
Anticipated Start: TBD
Expected Completion: TBD

Task Name: Disrupt the Attacker Ecosystem Through Transparency and Traceability
Action Number: 4.4
Task Summary: The ecosystem for automated, distributed threats favors the attacker. This task develops methods to disrupt ecosystems that are traditionally exploited to launch botnets, such as the gaming community, and increase risk to attackers through transparency and accountability. Industry and government jointly advocate within the relevant multistakeholder fora for wider implementation of measures that disrupt attacker tools and incentives.
Contributor(s): ICANN, RIRs, NTIA, Law Enforcement, FTC
Prerequisite Tasks: N/A
Anticipated Start: TBD
Expected Completion: TBD

Technology Development and Transition Line of Effort

The Technology Development and Transition Line of Effort has three complementary workstreams:

- Establishing a secure software marketplace
- International coordination
- Research and development

Technology Development and Transition Workstream 1: Establishing a Secure Software Marketplace

This series of tasks establishes 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.

Task Name: Establish Secure Software Development Lifecycle Guidelines
Action Number: 1.3
Task Summary: In collaboration with industry, NIST defines secure software development lifecycle guidelines for publication as a NIST Special Publication.
Contributor(s): NIST (Lead), DHS, industry
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: 2Q20

Task Name: Develop Guidelines for Software Component Transparency
Action Number: 1.3
Task Summary: Explore how manufacturers and vendors can communicate useful and actionable information about the third-party software components in modern software and IoT devices, and how this data can be used by enterprises to foster better security decisions and practices.
Contributor(s): NTIA (Lead), critical infrastructure sectors, digital ecosystem stakeholders
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: 2Q19

Task Name: Fill Gaps in Software Development Tools
Action Number: 1.3
Task Summary: The Networking and Information Technology Research and Development (NITRD) Program will promote targeted research funding and collaborative technology transition activities for software development tools required to efficiently and effectively adopt the secure software development lifecycle (SSDLC).
Contributor(s): NITRD (Lead)
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: 1Q23

Task Name: Enhance Software Development Toolchains

Action Number: 1.3
Task Summary: Accelerate development and adoption of effective and efficient software development techniques by managing an open competition for software development toolchains.
Contributor(s): NIST (Lead), DHS
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: 1Q22

Task Name: Showcase Advances in Secure Coding Practices and Share Information about Security Risks
Action Number: 5.3
Task Summary: Showcase advances in secure coding practices and tools developed by academia and security researchers and share information about security risks in the annual PrivacyCon conference.
Contributor(s): FTC (Lead)
Prerequisite Tasks: N/A
Anticipated Start: 3Q19
Expected Completion: Ongoing

Task Name: Agencies Require Secure Development for Government Off-the-Shelf (GOTS) Software
Action Number: 2.3
Task Summary: Federal procurement regulations are established for GOTS software development contracts that encourage or mandate application of the SSDLC.
Contributor(s): GSA, OMB, DOD, other U.S. departments and agencies
Prerequisite Tasks: Define core security capability baseline
Anticipated Start: TBD
Expected Completion: TBD

Task Name: Agencies Procure Securely Developed Commercial Off-the-Shelf (COTS) Software
Action Number: 2.3
Task Summary: Federal procurement regulations are established for COTS software procurement that prefer or require development using the SSDLC.
Contributor(s): GSA (Lead), OMB, DHS (Continuous Diagnostics and Mitigation Program), DOD, other U.S. departments and agencies
Prerequisite Tasks: Define core security capability baseline
Anticipated Start: TBD
Expected Completion: TBD

Task Name: Develop Best Practices for End-of-Life Software
Action Number: 1.5
Task Summary: Develop a range of end-of-life processes for dead and orphaned software and devices that balance customer and business requirements.
Contributor(s): CTA, NTIA, other government and industry participants
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: 4Q19

Technology Development and Transition Workstream 2: International Coordination

Task Name: Improve Existing U.S. Government Coordination on International Standards
Action Number: 4.2
Task Summary: Build on work of the Interagency International Cybersecurity Standardization Working Group (IICSWG) to further improve USG coordination in engagement with international standards bodies. Identify strategies for the promotion of industry-driven standards development within those bodies.
Contributor(s): NIST (lead), IICSWG member agencies
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: Ongoing

Task Name: Optimize Industry-USG Standards Coordination
Action Number: 4.2
Task Summary: Establish a framework and strategy for continuing coordination between U.S. industry entities and federal agencies that participate in international standards development.
Contributor(s): NIST, NTIA, State, IICSWG, industry, CSDE, trade associations
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: Ongoing

Task Name: Promote International Adoption of Best Practices Through Bilateral and Multilateral International Engagement
Action Number: 4.2
Task Summary: Promote adoption of internationally recognized best practices through bilateral, multilateral, and multistakeholder engagement, leveraging the expertise within USG agencies.
Contributor(s): State, NTIA, NIST, industry, civil society
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: TBD

Task Name: Promote awareness and adoption of specific established tools, protocols, and best practices at a global scale
Action Number: 3.3
Task Summary: Promote the implementation and adoption of established tools, protocols, and best practices that address automated cyber risks at scale. Develop easy-to-understand implementation guides, and work with stakeholders around the world. Develop the capacity to measure the impact of this implementation.
Contributor(s): Global Cyber Alliance, industry coordination bodies, NTIA, NIST, DHS
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: Ongoing

Task Name: Promote Best Practices for DNS Internationally
Action Number: 4.2
Task Summary: Promote best practices and relevant tools for DNS through U.S. positions at multistakeholder fora, such as ICANN, the IETF and the Internet Governance Forum.

Contributor(s): NTIA (Lead), government and private-sector multistakeholder participants
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: Ongoing

Technology Development and Transition Workstream 3: Research and Development

The rapid growth in DDoS capacity offered by IoT-based botnets imperils the effectiveness of current DDoS mitigation techniques. Research and development in techniques that offer mitigation closer to the source—or leverage new data analytics, machine learning, or artificial intelligence—are urgently needed to get ahead of malicious actors. Industry-led research activities are needed to develop and deploy innovative technologies. As a key source of funding for basic research in cybersecurity, the federal government should support this action through targeted funding and collaborative technology transition activities.

Task Name: Accelerate Federally Funded R&D for Mitigating Distributed Threats
Action Number: 1.4
Task Summary: Promote targeted research funding and collaborative technology transition activities for technologies that mitigate automated distributed threats.
Contributor(s): NITRD (Lead), DHS, U.S. departments and agencies
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: Ongoing

Task Name: Expedite Development and Deployment of Innovative Technologies for Prevention and Mitigation of Distributed Threats
Action Number: 1.4
Task Summary: Industry, academia, and government should expedite the development and deployment of innovative technologies for prevention and mitigation of distributed threats.
Contributor(s): Ecosystem players in a competitive environment
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: Ongoing

Task Name: Increase Accountability in Traffic Management
Action Number: 2.5
Task Summary: Examine the extent to which inter-autonomous system, internetwork peering, and transit agreements might improve traffic management accountability.
Contributor(s): NOGs, federal technology incubators, DHS, civil society, academia
Prerequisite Tasks: N/A
Anticipated Start: TBD
Expected Completion: TBD

Task Name: Accelerate Industry R&D for Mitigating Distributed Threats
Action Number: 1.4
Task Summary: Expedite the development and deployment of innovative technologies for prevention and mitigation of distributed threats.
Contributor(s): Industry consortia and labs, academia

Prerequisite Tasks: N/A
Anticipated Start: TBD
Expected Completion: TBD

Task Name: Prioritize Technology Transition
Action Number: 2.5
Task Summary: Emphasize technology transition strategies as a key component of research plans for new tools and practices for network traffic management.
Contributor(s): Coalition TBD of industry, government, and civil society
Prerequisite Tasks: N/A
Anticipated Start: TBD
Expected Completion: TBD

Task Name: Promote Emerging Best Practices
Action Number: 1.4
Task Summary: Amplify research and technology transition efforts as technologies mature and best practices emerge.
Contributor(s): Civil society TBD
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: Ongoing

Awareness and Education Line of Effort

The Awareness and Education Line of Effort has two complementary workstreams:

- Promote consumer confidence
- Educate the workforce

Awareness and Education Workstream 1: Promote Consumer Confidence

Consumers' lack of confidence in the security of IoT devices may be hindering IoT adoption. This series of tasks 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.

Task Name: Promote Appropriate Product Deployment
Action Number: 4.3
Task Summary: Educate consumers on different baselines and assessment programs that will show that deployed products are using appropriate security.
Contributor(s): Sector-specific agencies, civil society, consumer groups, FTC, DHS, NTIA, CTA
Prerequisite Tasks: Establish assessment program for Home IoT devices; establish assessment program for industrial IoT devices; specify IoT security capability baseline
Anticipated Start: 1Q20
Expected Completion: 3Q23

Task Name: Deter Illegal Marketing Practices
Action Number: 4.3

Task Summary: Halt and deter illegal marketing practices by IoT and IT vendors through enforcement actions.
Contributor(s): FTC (lead)
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: Ongoing

Task Name: Mitigating IoT-based DDoS
Action Number: 1.5
Task Summary: Demonstrate the impact and practicality of combining manufacturer usage descriptions (MUD), threat signaling, secure updates, and basic cyber hygiene to protect IoT devices and mitigate the impact of compromised IoT devices.
Contributor(s): NIST (Lead), civil society, Internet engineers
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: Ongoing

Awareness and Education Workstream 2: Educating the Workforce

As a full range of products and services comes online, cybersecurity threats arise in new classes of products. Product designers are deeply steeped in traditional risks associated with their products, but are often unaware of the new risks that can be introduced when the products are connected to the network. This series of tasks focuses on educating the existing and emerging workforce, regardless of engineering discipline, on basic cybersecurity.

Task Name: Prepare the Programming Workforce
Action Number: 1.3
Task Summary: Incorporate secure-by-design principles and supporting tools in programming courses throughout the course of study.
Contributor(s): Academia, secure software development community, training and certification providers, accreditation bodies, government
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: 2Q20

Task Name: Prepare the Engineering Workforce
Action Number: 5.4
Task Summary: Incorporate cybersecurity principles in course of study for all engineering disciplines.
Contributor(s): Academia, federal and state governments
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: 2Q20

Task Name: Align Curriculum with Workforce Needs
Action Number: 5.3

Task Summary: Continue to promote the National Initiative for Cybersecurity Education (NICE) Framework as a reference tool for the development of course content, particularly with respect to software development.
Contributor(s): NIST (Lead), Academia, accreditation bodies, professional societies, certification providers
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: 4Q18

Task Name: Establish Cybersecurity Educational Program for Engineers
Action Number: 5.4
Task Summary: Establish cybersecurity as a fundamental requirement across all engineering disciplines, and create or leverage existing online cybersecurity training for engineers.
Contributor(s): NIST, cybersecurity education community, accreditation programs
Prerequisite Tasks: N/A
Anticipated Start: In progress
Expected Completion: 1Q21

III. Next Steps

The Departments of Commerce and Homeland Security will work with other U.S. government agencies and the private sector to coordinate and track road map activities. DHS will coordinate across sector-specific agencies and with critical infrastructure organizations. Commerce will coordinate standards and technical activities through NIST, and will coordinate across government and the digital economy through NTIA.

We will also provide updates periodically, including:

- Meeting and communicating regularly with private-sector stakeholders who are leading key initiatives to share information and progress.
- Convening stakeholders at the mid-term (approximately six months after road map publication), through a workshop or other session, to discuss progress on road map implementation.
- Providing a 365-day status report to the President on implementation, due one year after publication of the final road map, as detailed in the Botnet Report. This update will review progress of the community as a whole, will reassess the threat to the extent practicable, and will discuss key activities in the coming year.

As discussed in the Botnet Report and in Section II of this document, the problem of automated, distributed attacks cannot be solved by a single entity, and will require action, coordination and the harnessing of innovation across government and the private sector (including industry, academia, and civil society). The Departments look forward to working with the private sector and other government entities over the coming year and beyond to improve the security of the Internet ecosystem.