A Report to the President

on

Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats

---

Transmitted by
The Secretary of Commerce
and
The Secretary of Homeland Security

May 22, 2018

Table of Contents

Executive Summary

This report responds to the May 11, 2017, Executive Order, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." That order 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 Departments of Commerce and Homeland Security worked jointly on this effort through three approaches—hosting two workshops, publishing two requests for comment, and initiating an inquiry through the President's National Security Telecommunications Advisory Committee (NSTAC)—aimed at gathering a broad range of input from experts and stakeholders, including private industry, academia, and civil society. These activities all contributed to the information-gathering process for the agencies developing the recommendations in this report.

The Departments worked in consultation with the Departments of Defense, Justice, and State, the Federal Bureau of Investigation, the sector-specific agencies, the Federal Communications Commission and Federal Trade Commission, and other interested agencies.

The Departments determined that the opportunities and challenges in working toward dramatically reducing threats from automated, distributed attacks can be summarized in six principal themes.

1. **Automated, distributed attacks are a global problem.** The majority of the compromised devices in recent noteworthy botnets have been geographically located outside the United States. To increase the resilience of the Internet and communications ecosystem against these threats, many of which originate outside the United States, we must continue to work closely with international partners.
2. **Effective tools exist, but are not widely used.** While there remains room for improvement, the tools, processes, and practices required to significantly enhance the resilience of the Internet and communications ecosystem are widely available, and are routinely applied in selected market sectors. However, they are not part of common practices for product development and deployment in many other sectors for a variety of reasons, including (but not limited to) lack of awareness, cost avoidance, insufficient technical expertise, and lack of market incentives.
3. **Products should be secured during all stages of the lifecycle.** Devices that are vulnerable at time of deployment, lack facilities to patch vulnerabilities after discovery, or remain in service after vendor support ends make assembling automated, distributed threats far too easy.
4. **Awareness and education are needed.** Home users and some enterprise customers are often unaware of the role their devices could play in a botnet attack and may not fully understand the merits of available technical controls. Product developers, manufacturers, and infrastructure operators often lack the knowledge and skills necessary to deploy tools, processes, and practices that would make the ecosystem more resilient.
5. **Market incentives should be more effectively aligned.** Market incentives do not currently appear to align with the goal of "dramatically reducing threats perpetrated by automated and distributed attacks." Product developers, manufacturers, and vendors are motivated to minimize cost and time to market, rather than to build in security or offer efficient security updates. Market incentives must be realigned to promote a better balance between security and convenience when developing products.

6. **Automated, distributed attacks are an ecosystem-wide challenge.** No single stakeholder community can address the problem in isolation.

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. A list of suggested actions for key stakeholders reinforces each goal. The goals are:

- Goal 1: Identify a clear pathway toward an adaptable, sustainable, and secure technology marketplace.
- Goal 2: Promote innovation in the infrastructure for dynamic adaptation to evolving threats.
- Goal 3: Promote innovation at the edge of the network to prevent, detect, and mitigate automated, distributed attacks.
- Goal 4: Promote and support coalitions between the security, infrastructure, and operational technology communities domestically and around the world.
- Goal 5: Increase awareness and education across the ecosystem.

The recommended actions and options include ongoing activities that should be continued or expanded, as well as new initiatives. No single investment or activity can mitigate all threats, but organized discussions and stakeholder feedback will allow us to further evaluate and prioritize these activities based on their expected return on investment and ability to measurably impact ecosystem resilience. This report calls for a status update that will evaluate the level of progress made by stakeholders in countering automated, distributed threats.

This effort will not end with the publication of this report. There is much work to do. However, we do not expect all actions to occur simultaneously, due to considerations such as resource constraints in the relevant stakeholder communities. In addition, some actions are already in progress, while others are dependent on outside factors. We propose a model to support coordination and collaboration for implementing the actions described in Section III, with a particular emphasis on federal requirements. While some actions directly related to the federal government are clearly appropriate for the government to lead, this model provides a way for stakeholders to collaborate with government as they move forward on those actions that are best accomplished through private-sector leadership.

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 Secretary of Commerce and 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)."

These types of attacks have been a concern since the early days of the Internet,[2] and were a regular occurrence by the early 2000s.[3] Automated and distributed attacks form a threat that reaches beyond any single company or sector. These threats are used for a variety of malicious activities, including distributed denial of service (DDoS) attacks that overwhelm networked resources, sending massive quantities of spam, disseminating keylogger and other malware; ransomware attacks distributed by botnets that hold systems and data hostage; and computational propaganda campaigns[4] that manipulate and intimidate communities through social media. Traditional DDoS mitigation techniques, such as network providers building in excess capacity to absorb the effects of botnets, are designed to protect against botnets of an anticipated size. With new botnets that capitalize on the sheer number of "Internet of Things" (IoT) devices,[5] DDoS attacks have grown in size to more than one terabit per second, far outstripping expected size and excess capacity. As a result, recovery time from these types of attacks may be too slow, particularly when mission-critical services are involved. Further, these mitigation techniques were not designed to remedy other classes of malicious activities facilitated by botnets, such as ransomware or computational propaganda.

As new scenarios emerge, there is an urgent need for coordination and collaboration across a diverse set of stakeholders. The federal government has worked with stakeholders in the past to address new threats as they arise. Previous efforts include the Industry Botnet Group, which led to the Principles for Voluntary Efforts to Reduce the Impact of Botnets in Cyberspace (2012);[6] information sharing and coordination efforts of the financial services sector following the DDoS attacks on banks in 2012 and

[1] Exec. Order No. 13,800, 82 Fed. Reg. 22,391 (May 11, 2017), *available at* https://www.federalregister.gov/d/2017-10004.
[2] United States v. Morris, 928 F.2d 504 (2d Cir. 1991).
[3] *See, e.g.*, Stuart Staniford, Vern Paxson & Nicholas Weaver, *How to 0wn the Internet in Your Spare Time*, Proceedings of the 11th USENIX Security Symposium, San Francisco, CA, Aug. 5-9, 2002, *available at* https://www.usenix.org/legacy/event/sec02/full_papers/staniford/staniford.pdf.
[4] Computational propaganda is the "assemblage of social media platforms, autonomous agents, and big data tasked with the manipulation of public opinion." Samuel C. Woolley & Philip N. Howard, *Political Communication, Computational Propaganda, and Autonomous Agents—Introduction*, 10 Int'l Journal of Commc'n 4882, 4886 (2016), *available at* http://ijoc.org/index.php/ijoc/article/viewFile/6298/1809.
[5] Examples of IoT devices include (but are not limited to) connected lightbulbs, door locks, parking meters, personal health monitors, industrial automation and sensors, and automobiles.
[6] Industry Botnet Group, *Principles for Voluntary Efforts to Reduce the Impact of Botnets in Cyberspace*, https://archive.is/20131015084520/www.industrybotnetgroup.org/principles/ (last visited Apr. 4, 2018).

2013;[7] the Communications Security, Reliability and Interoperability Council's (CSRIC)[8] Anti-Bot Code of Conduct (2013),[9] and reports on Internet Service Provider (ISP) Network Protection Practices (2010)[10] and Remediation of Server-Based DDoS Attacks (2014);[11] and the active and ongoing work by the Department of Justice and its many partners on addressing and "sink-holing" the infrastructure supporting these threats.[12] While these initiatives have made some progress, the impacts have been incremental, and significant challenges remain. By proactively addressing these challenges, this Administration and key stakeholders have an opportunity to enhance the resilience of the future Internet and communications ecosystem.

The DDoS attacks launched from the Mirai botnet in the fall of 2016, for example, reached a level of sustained traffic that overwhelmed many common DDoS mitigation tools and services, and even disrupted a Domain Name System (DNS) service that was a commonly used component in many DDoS mitigation strategies.[13] This attack also highlighted the growing insecurities in—and threats from—consumer-grade IoT devices. As a new technology, IoT devices are often built and deployed without important security features and practices in place.[14] While the original Mirai variant was relatively simple, exploiting weak device passwords, more sophisticated botnets have followed; for example, the Reaper botnet uses known code vulnerabilities to exploit a long list of devices,[15] and one of the largest DDoS attacks seen to date recently exploited a newly discovered vulnerability in the relatively obscure

---

[7] *Evaluating the Security of the U.S. Financial Sector: Hearing Before the Task Force to Investigate Terrorism Financing*, House Committee on Financial Services, 114th Cong. 40-59 (2015) (statement of John W. Carlson, Chief of Staff, Financial Services Information Sharing and Analysis Center (FS-ISAC)), *available at* https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg96997/pdf/CHRG-114hhrg96997.pdf.

[8] CSRIC is an advisory committee of the Federal Communications Commission, the mission of which is to make recommendations to the Commission to promote the security, reliability, and resilience of the nation's communications systems. For more information, including past security efforts, see CSRIC, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0 (last visited Apr. 4, 2018).

[9] Communications Security, Reliability and Interoperability Council III Working Group 7, *Final Report on U.S. Anti-Bot Code of Conduct (ABC) for Internet Services Providers (ISPs)*, (Mar. 2013), *available at* https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf.

[10] Communications Security, Reliability and Interoperability Council Working Group 8, *Final Report on Internet Service Provider (ISP) Network Protection Practices*, (Dec. 2010), *available at* http://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf.

[11] Communications Security, Reliability and Interoperability Council IV Working Group 5, *Final Report on Remediation of Server-Based DDoS Attacks*, (Sept. 2014), *available at* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG5_Remediation_of_Server-Based_DDoS_Attacks_Report_Final_(pdf)_V11.pdf.

[12] *See, e.g.*, U.S. Department of Justice, *Avalanche Network Dismantled in International Cyber Operation*, (Dec. 5, 2016), https://www.justice.gov/opa/pr/avalanche-network-dismantled-international-cyber-operation.

[13] United States Computer Emergency Readiness Team, *Alert (TA16-288A): Heightened DDoS Threat Posed by Mirai and Other Botnets*, https://www.us-cert.gov/ncas/alerts/TA16-288A (last revised Oct. 17, 2017).

[14] The National Security Telecommunications Advisory Committee, *NSTAC Report to the President on the Internet of Things*, (Nov. 19, 2014), *available at* https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf.

[15] Brian Krebs, *Fear the Reaper, or Reaper Madness?* Krebs on Security (Oct. 27, 2017, 4:39 PM), https://krebsonsecurity.com/2017/10/fear-the-reaper-or-reaper-madness/.

MemCacheD software.[16] These examples clearly demonstrate the risks posed by botnets of this size and scope, as well as the expected innovation and increased scale and complexity of future attacks.

Approach

The Departments of Commerce and Homeland Security worked jointly on this effort through three approaches aimed at gathering a broad range of input from experts and stakeholders, including private industry, academia, and civil society. The Departments worked in consultation with the Departments of Defense, Justice, and State, the Federal Bureau of Investigation, the sector-specific agencies, the Federal Communications Commission, and the Federal Trade Commission, as well as other interested agencies.

In June 2017, Commerce's National Telecommunications and Information Administration (NTIA) issued a Request for Comment (RFC) on "Promoting Stakeholder Action Against Botnets and Other Automated Threats."[17] The RFC asked for feedback on "current, emerging, and potential approaches for dealing with botnets and other distributed, automated attacks." NTIA received 47 comments, with respondents ranging from large trade associations (representing thousands of companies) to individual technical experts. The commenters also represented a diverse range of industries and sectors, including Internet service providers, security firms, infrastructure providers, software manufacturers, civil society, and academia from both U.S. and non-U.S. organizations.

In July 2017, Commerce's National Institute of Standards and Technology (NIST) hosted a workshop on "Enhancing Resilience of the Internet and Communications Ecosystem."[18] The workshop encouraged stakeholders to explore current and emerging solutions addressing automated, distributed threats in an open and transparent manner. It attracted 150 participants from diverse stakeholder communities, who identified a broad range of coordinated actions by all stakeholders to address these threats.

As directed in Executive Order 13800, a draft report was published in January 2018, followed by a second RFC and workshop, at which stakeholders discussed substantive public comments and next steps. These activities contributed to the information-gathering process for agencies developing the recommendations in this final report. The comments and workshop discussions will also inform many of the actions that will take place after this report is published.

The Department of Homeland Security's (DHS) participation in this effort was focused through the President's National Security Telecommunications Advisory Committee's (NSTAC) Internet and Communications Resilience subcommittee, which finalized and approved the *NSTAC Report to the*

[16] Lili Hay Newman, *GitHub Survived the Biggest DDoS Attack Ever Recorded*, Wired (Mar. 1, 2018, 11:01 AM), https://www.wired.com/story/github-ddos-memcached/.

[17] Additional information, including the public comments, is available at National Telecommunications and Information Administration, *Request for Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats*, (June 8, 2017), https://www.ntia.doc.gov/federal-register-notice/2017/rfc-promoting-stakeholder-action-against-botnets-and-other-automated-threats.

[18] National Institute of Standards and Technology, *Enhancing Resilience of the Internet and Communications Ecosystem*, https://www.nist.gov/news-events/events/2017/07/enhancing-resilience-internet-and-communications-ecosystem (last updated July 10, 2017). For a summary of the proceedings, see Tim Polk, *Enhancing Resilience of the Internet and Communications Ecosystem: A NIST Workshop Proceedings*, (Sept. 2017), NIST Interagency/Internal Report No. 8192, *available at* http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8192.pdf.

President on Internet and Communications Resilience on November 16, 2017.[19] While developing its report, the NSTAC studied botnets, as well as forms of attacks that may be facilitated by botnets, such as DDoS attacks and vectors that could be used to create botnets (*i.e.*, end user devices and IoT). Through its study, the NSTAC concluded that automated and distributed attacks facilitated through botnets threaten the security and resilience of the Internet and communications ecosystem, and in turn, the nation's critical infrastructure. Additionally, the NSTAC determined that compromised IoT devices will increasingly be used by malicious actors to launch global automated attacks.

Principal Themes

The opportunities and challenges we face in working toward dramatically reducing threats from automated, distributed attacks can be summarized in six principal themes.

1. **Automated, distributed attacks are a global problem.** The majority of the compromised devices in recent noteworthy botnets have been geographically located outside the United States. To increase the resilience of the Internet and communications ecosystem against these threats, many of which originate outside the United States, we must continue to work closely with international partners.
2. **Effective tools exist, but are not widely used.** While there remains room for improvement, the tools, processes, and practices required to significantly enhance the resilience of the Internet and communications ecosystem are widely available, and are routinely applied in selected market sectors. However, they are not part of common practices for product development and deployment in many other sectors for a variety of reasons, including (but not limited to) lack of awareness, cost avoidance, insufficient technical expertise, and lack of market incentives.
3. **Products should be secured during all stages of the lifecycle.** Devices that are vulnerable at time of deployment, lack facilities to patch vulnerabilities after discovery, or remain in service after vendor support ends make assembling automated, distributed threats far too easy.
4. **Awareness and education are needed.** Home users and some enterprise customers are often unaware of the role their devices could play in a botnet attack and may not fully understand the merits of available technical controls. Product developers, manufacturers, and infrastructure operators often lack the knowledge and skills necessary to deploy tools, processes, and practices that would make the ecosystem more resilient. Customer-friendly mechanisms to identify more secure choices analogous to programs such as the Energy Star program[20] or National Highway Traffic Safety Administration (NHTSA) 5- Star Safety Ratings[21] are needed to increase consumer awareness and inform buying decisions.
5. **Market incentives should be more effectively aligned.** Market incentives do not currently appear to align with the goal of "dramatically reducing threats perpetrated by automated and distributed attacks." Product developers, manufacturers, and vendors are motivated to minimize cost and time to market, rather than to build in security or offer efficient security

[19] The National Security Telecommunications Advisory Committee, *NSTAC Report to the President on Internet and Communications Resilience*, (Nov. 16, 2017), *available at* https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR%20FINAL%20%2810-12-17%29%20%281%29-%20508%20compliant_0.pdf.

[20] Energy Star, *About Energy Star*, https://www.energystar.gov/about (last visited Apr. 4, 2018).

[21] National Highway Traffic Safety Administration, *Search NHTSA's 5-Star Safety Ratings*, https://www.safercar.gov/Vehicle-Shoppers (last visited Apr. 4, 2018).

updates. Market incentives must be realigned to promote a better balance between security and convenience when developing products.

6. **Automated, distributed attacks are an ecosystem-wide challenge.** No single stakeholder community can address the problem in isolation.

A Note About Threats

This paper does not differentiate between nation-states, cyber-criminals, and other threat actors. While some attacks may be difficult to initially attribute, the ecosystem still must come together to mitigate an attack. This open and transparent process focused on areas that would elicit the widest participation from stakeholders across the Internet and communications ecosystem regarding security improvements, as well as cooperation before, during, and after attacks, understanding that the identity of a given threat actor may be initially unknown. The 2018 Worldwide Threat Assessment of the U.S. Intelligence Community released by the Office of the Director of National Intelligence provides insight into the cyber threat landscape.[22] Though beyond the scope of this report, it will be important to differentiate between nation-state, cyber-criminal, and other threat actors in determining how to best apply a broad range of threat-specific U.S. government authorities. Some workshop participants also recognized their limitations in addressing specific classes of threat actors. Future attention should be placed on these issues, engaging broader ecosystem stakeholders as appropriate.

II. Current Status of the Ecosystem and Vision for the Future

This section describes the current status of the technical and policy domains of the Internet and worldwide communications ecosystem, and envisions an improved future. The technical domains of the ecosystem include:

- The ***infrastructure*** that connects the other technical domains into a single system;
- ***Enterprise networks*** composed of locally connected devices with Regional Internet Registry (RIR)[23]-assigned Internet Protocol (IP) version 4 (IPv4) and IPv6 Internet addresses and locally connected sub-local area networks (LANs) using private IP address space or alternative protocols (*e.g.*, Bluetooth Low Energy);
- ***Edge devices*** such as personal computers, mobile devices, edge servers, and IoT and other connected devices; and
- ***Home and small business networks*** composed of devices using private IP address space addressable externally through network address translation (NAT).

The policy domain is intertwined with the technical domains, and includes:

- **Public-private partnerships**, including information-sharing arrangements;

[22] *See* Daniel R. Coats, Director of National Intelligence, *Worldwide Threat Assessment of the US Intelligence Community*, Statement for the Record at the Senate Select Committee on Intelligence, (Feb. 13, 2018), *available at* https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

[23] "Regional Internet Registries (RIRs) are nonprofit corporations that administer and register Internet Protocol (IP) address space and Autonomous System (AS) numbers within a defined region." American Registry for Internet Numbers, *Regional Internet Registries*, https://www.arin.net/knowledge/rirs.html (last visited Apr. 4, 2018).

- **Voluntary attestation or certification processes**, where vendors and customers opt-in to shared security goals and expectations;
- **Standards and guidelines** developed in multistakeholder fora;
- **Procurement policies**, especially within the federal government, to create market incentives;
- **Regulatory and legislative actions** at the federal and/or state levels; and
- **International engagement** to build on shared goals and best practices.

Improved resilience against automated, distributed attacks will require collaboration on technical, policy, and other solution sets across nations, sectors, and technical layers. Effective policies will provide clear expectations for use of standards and guidelines that remain flexible and adaptable as the security risk evolves. No single solution or framework will address every risk, but better collaboration across the domains will improve the ability of ecosystem members to mitigate the botnet threat.

Technical Domains

Infrastructure: Current State

In the face of automated, distributed attacks, the current infrastructure underlying the digital ecosystem has demonstrated remarkable resilience, but the increasing size and scope of attacks appear to be testing the limits of that resilience. These two perspectives arose after the 2016 Mirai botnet attacks that temporarily interrupted services of an Internet infrastructure provider, disrupting many major online services and websites in North America and Europe. However, the disruptions were temporary, and key players responded quickly. This response underscores both the interdependence of the infrastructure, and the ability of individuals and organizations to learn and adapt quickly.

In this report, "infrastructure" includes the technology and organizations that enable connectivity, interoperability, and stability, going beyond the physical wires, wireless transmitters and receivers, and satellite links to include the hardware, software, tools, standards, and practices on which the ecosystem depends—for example, routers, switches, Internet service providers, DNS providers, content delivery networks, hosting and cloud-service providers.[24] Because of the complexity of modern infrastructure, with key tools and players interspersed through the ecosystem, no single tool can secure the infrastructure. Traditionally, as new threats emerge, particular subsets of infrastructure players work together to understand the risk and the path to mitigation.

Filtering traffic as it enters and exits a network—the technique known as ingress and egress filtering—is one such tool. IP-spoofing is a common technique employed in DDoS attacks, where the attacker fabricates the source IP address to prevent the victim from filtering bad traffic by the traffic's origin. Network providers can limit spoofing by restricting incoming traffic to that which is actually originating from its stated network, filtering out traffic that claims to come from outside its expected network space.[25] Ingress filtering is acknowledged to be a longstanding best practice by the Internet Engineering

[24] While Presidential Policy Directive (PPD) 21 recognizes the systems and assets of the communications and information technology sectors as critical infrastructure, this document uses the term "Internet infrastructure" to additionally encompass the organizations and practices upon which the Internet ecosystem depends.
[25] DHS is developing and supporting open source software tools to assess and report on the deployment of source address validation (SAV) best anti-spoofing practices. For more information, see Center for Applied Internet Data Analysis, *Spoofer*, https://www.caida.org/projects/spoofer/.

Task Force (IETF) and other infrastructure-focused organizations.[26] It can be complemented by egress filtering, in which an organization or network operator deploys filters at the edge of its network to prevent traffic that does not appear to originate from inside the network from exiting onto the global Internet.

Major domestic carriers implement the ingress filtering standards in at least some portion of their networks. However, these standards are not universally supported worldwide, or by smaller domestic infrastructure providers. Many technical and business experts have objected to proposals to apply ingress filtering higher up in the Internet, at the level of international backbones, because it would be more likely to block legitimate traffic.[27] Egress filtering is advocated as a common security practice for enterprises,[28] but is still uncommon for small and medium-sized enterprises. Although not universally implemented, network ingress/egress filtering, where implemented, is effective at mitigating the class of DDoS attacks that leverage IP-source address spoofing.

Infrastructure providers and other companies offer commercial anti-DDoS services, which can play a key role in limiting the impacts of attacks against particular targets. However, not all enterprise customers purchase the full slate of anti-DDoS services, due to the expense and the complexity of integrating those services into the other components of the enterprise's network. Meanwhile, attackers quickly learn to exploit holes in existing services. When confronted by attacks that rely on the sheer volume of traffic, off-premise DDoS mitigation solutions either provision more network capacity or use the shape of the network itself to limit the volume of traffic that reaches the target. Other attacks target the web server or application itself. An enterprise's on-premise devices and tools detect and filter these attacks on the target network.

The current best practices involve employing a hybrid approach that uses both local filtering and DDoS defense tools that increase off-premise capacity. However, implementing best practices can be expensive, difficult to manage, and require skilled staff. These best practices are also typically built around past crises, making it difficult, for example, to argue for a large amount of excess capacity until under attack. An active threat detection program that detects vulnerabilities and attack trends can supplement these efforts, helping the victim organization to respond as needed. Content delivery networks (CDNs) are another tool that can leverage large, dedicated private infrastructures to protect customers. As different attacks emerge, or adversaries select new targets, organizations often invest in threat-specific defenses.

Responding in a timely fashion requires preparation and knowledge. Given the large set of security controls needed in the modern Internet, not all staff at smaller infrastructure providers or key enterprises are aware of the benefits of filtering and other tools. Many infrastructure providers offer warnings about compromises and ongoing attacks, but if enterprises ignore those warnings, then the infrastructure provider is less likely to diligently follow up with further warnings. Victims often struggle

[26] *See*, *e.g.*, P. Ferguson & D. Senie, *Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing*, (May 2000), Internet Engineering Task Force – Network Working Group, *available at* https://tools.ietf.org/html/bcp38 ("BCP 38"); and F. Baker & P. Savola, *Ingress Filtering for Multihomed Networks*, (Mar. 2004), Internet Engineering Task Force – Network Working Group, *available at* https://tools.ietf.org/html/bcp84 ("BCP 84").

[27] Packets may be routed between Internet endpoints via significantly different paths at different instances in time for legitimate reasons.

[28] *See*, *e.g.*, Chris Brenton, *Egress Filtering FAQ*, SANS Institute, https://www.sans.org/reading-room/whitepapers/firewalls/egress-filtering-faq-1059 (last revised Apr. 19, 2006).

when encountering their first substantial attack without a response plan in place, because they depend on the very network under attack to understand it and contact service providers for aid.

Vision for the Future of Infrastructure

Infrastructure providers of all types must develop a broad understanding of the benefits of shared defense approaches, and communities should work together to drive best-practice adoption. This work includes ubiquitous adoption of filtering at the interface with customer networks, including multi-tenant infrastructures such as cloud providers. Ideally, infrastructure providers should understand the current levels of attacks, maintain sufficient capacity to absorb realistically expected levels of malicious traffic, and communicate those capabilities to their customers. Infrastructure-provider services for DDoS mitigation should integrate with customers' existing network solutions, regardless of the level of service a customer has chosen.

As new products and tools become available, players across the ecosystem should understand how their behavior can help—or hinder—their efficacy. An increasingly smart network can segment different types of traffic automatically, to isolate or mitigate applications or devices that are sources and targets of attacks. Enterprises are increasingly able to address application-level attacks with appropriate tools, and the vendors of these tools should work with both customers and the relevant application vendors to make security decisions easier and more efficient.

Increased implementation of a number of existing technologies will help mitigate these attacks. Some of the existing infrastructure is built on older protocols, such as the IPv4 network and legacy routing protocols. Broader adoption of current standards and best practices will bring security benefits. For example, the IPv6 network can better enable device-specific recognition across the network to detect device-level aberrant behavior.[29] Small and medium-sized organizations should incorporate industry best practices, and, as new infrastructure standards and practices are needed and proven, infrastructure providers should efficiently adopt them.

At the core of the infrastructure, key players already share information about the evolving nature of threats. While many of these organizations employ experts who coordinate with their peers around the globe, in the future, information sharing must expand to include smaller, less well-funded, or niche players through new automated tools and practices. Incentives could promote investment in better, more efficient detection of malicious traffic, as well as more public commitments to avoid carrying malicious traffic. These commitments would build on existing relationships across the community to help build a more stable global network.

Enterprise Networks: Current State

Networks that support enterprises (*e.g.*, medium and large businesses, government agencies, and academic institutions) are another key technical domain in the Internet and communications ecosystem. These networks are often complex, with enterprise-owned and -operated Border Gateway Protocol (BGP) routers, DNS resolvers, and applications that rely on a mix of local and cloud-based services. Edge devices often include powerful servers, personal computing devices, mobile phones, and enterprise-managed and unmanaged IoT devices. Devices on enterprise networks can use a mixture of statically or

[29] The current IPv4 workaround, Network Address Translation (NAT), does offer firewalling benefits, especially at the home network level. However, it should be noted that, once IPv6 is implemented, attackers could identify specific addresses of targeted devices that would previously have been more difficult to recognize behind NAT. Experts have also expressed some concern about the security of some IPv6 implementations.

dynamically assigned addresses from one or more public IP address ranges (*e.g.*, addresses acquired from an RIR) as well as addresses assigned from locally administered private IP address ranges. The large presence of enterprise networks connected to the Internet means that they are not only potential victims but are also sources of risk.

Many well-known DDoS attacks, such as the attacks on U.S. banks in 2012 and 2013, targeted customer-facing services associated with large enterprises.[30] Just as the 2016 Mirai attacks allowed some enterprises to demonstrate resilience in the face of vulnerability, the 2012-2013 attacks spurred the financial sector and its partners to discover weaknesses and demonstrate paths to greater resilience. These attacks were disruptive, but the sector mitigated the effects of the attacks through increased investment in technology and resources, as well as active collaboration across the community, including their network service providers and technical partners, as well as with government. Organizations shared lessons learned as the attacks continued, and institutions such as the Financial Services Information Sharing and Analysis Center (ISAC) and the Financial Services Roundtable facilitated information sharing and coordination with the major ISPs. The scale of the attacks inspired leadership from the highest levels of management, and drove a more enduring relationship with government experts, as well as commitment to invest in tools and services.

Resources associated with enterprise networks are also a significant factor in executing automated, distributed threats. Devices at the enterprise level, ranging from IoT devices to data center servers, can be compromised and incorporated into botnets. Poorly administered enterprise resources, such as open DNS resolvers, are often leveraged to amplify attacks. For some enterprises, it can be a challenge to keep all systems and devices patched and updated across their global networks. Enterprise-operated routers that do not enforce ingress and egress filtering have facilitated attacks that featured address spoofing, allowing botnet participants to hide their true locations. In the case of cloud providers, enterprise resources have been rented (usually with stolen credit cards) to quickly assemble significant botnets. In many countries, the issues surrounding legacy systems are compounded by the widespread use of pirated software, which is typically not patched and is therefore vulnerable to known exploits. Enterprises with heavy use of pirated software are extremely difficult to protect, providing malicious actors with a reservoir of systems that are easily assembled into distributed threats.

Enterprises that have faced DDoS attacks, or that are from sectors broadly impacted by these attacks, often build potential attacks into their risk model and employ a mix of DDoS mitigations offered by infrastructure providers and enterprise-managed on-premise mitigations. Enterprises that understand the risks and implement these mechanisms are the exception. Many at-risk enterprises are unaware of the potential impacts of DDoS attacks on their operations. Such enterprises may not fully understand their ability to protect their networks and respond to and recover from an attack. For example, they may not understand the limitations of their contracts with infrastructure providers, or the availability of products and services to mitigate DDoS attacks. They also may not understand fully the cost to recover from such an attack.

In the absence of an ongoing attack, enterprises traditionally focus on availability, functionality, and cost. As a result of that focus, enterprises are likely to rely on legacy devices that can no longer be adequately secured, or will deploy IoT and other devices that were never designed to be secure. Where

[30] *See* David Goldman, *Major Banks Hit With Biggest Cyberattacks in History*, CNN (Sept. 28, 2012, 9:27 AM ET), http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html.

security updates are available, enterprises may have extremely onerous processes to evaluate patches or long periods between scheduled maintenance, expanding the window of vulnerability.[31]

While enterprises typically have professional information technology (IT) operations staff, cybersecurity-specific expertise is often lacking. This challenge is often compounded by a similar lack of awareness among organizations' decision makers, who are responsible for resourcing IT operations within their organizations or for overseeing the IT operations. IT operations teams are often unaware of the risks of open resolvers and other sources of attack amplification, or the importance of ingress and egress filtering. When ISPs, for example, report potential compromise to customers, ISPs often find that the enterprise cannot identify or locate the compromised devices, and even if the enterprise can identify and locate the devices, it may not have the tools or expertise to recover to a secure state. Enterprises may struggle to work collaboratively with service providers when under attack. Failure to implement basic backup procedures places enterprises at greater risk for a challenging recovery from ransomware distributed by botnets.

Enterprises can contribute to a more resilient ecosystem through a mix of current and emerging technologies, operational and procurement policies, and awareness and education for IT staff and decision makers.

Vision for the Future of Enterprise Networks

A foundational step toward this vision would be increased enterprise application of the principles contained in the NIST Cybersecurity Framework (CSF).[32] Most of the necessary actions can be ascribed to the five concurrent and continuous functions of the framework:

- **Identify.** Enterprises locate legacy devices and other devices that cannot be secured. Enterprises remove these high-risk devices from service wherever possible and replace them with devices that are inherently secure or can be secured.
- **Protect.** The system architecture provides additional layers of protection to any remaining high-risk devices (*e.g.*, access to legacy devices would be restricted by network architecture). Enterprises deploy or procure on- and off-premise DDoS mitigation services. Enterprises' network architectures limit exposure of devices to malicious actors and limit damage from compromised devices. Ingress and egress filtering are implemented to prevent network address spoofing, and attack amplifiers (*e.g.*, open resolvers) are reconfigured. Efficient update processes minimize the window of vulnerability for all devices on the network. Multi-tenant infrastructures also enforce ingress and egress filtering to reduce the impact of cloud-based botnets.
- **Detect.** A combination of ISP-based detection services and enterprise-operated network and service monitoring detect outbound malicious traffic, inbound attacks, and identify compromised devices in near real-time.
- **Respond.** Enterprises have policies and procedures to address compromised devices (*e.g.*, replace, mitigate, or patch a device participating in a botnet) when detected by the enterprise or

[31] *See* Dan Goodin, *Failure to Patch Two-month-old Bug Led to Massive Equifax Breach*, Ars Technica (Sept. 13, 2017), https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/. *See also* Federal Trade Commission, *Mobile Security Updates: Understanding the Issues* (Feb. 2018), https://www.ftc.gov/system/files/documents/reports/mobile-security-updates-understanding-issues/mobile_security_updates_understanding_the_issues_publication_final.pdf.

[32] National Institute of Standards and Technology, *Cybersecurity Framework*, https://www.nist.gov/cybersecurity-framework (last visited Apr. 4, 2018).

ISP. Enterprises also have processes in place to contact their ISP(s) or other anti-DDoS service providers when attacks are detected locally. Key operational resources continue to operate with constrained resources.

- **Recover.** Enterprises have the ability to reconstitute compromised systems (*e.g.*, from backup) rather than submit ransomware payments to resume operations.

The technologies and operational policies highlighted above are realistic only if supported by an appropriate mix of procurement policies and awareness and education initiatives. Enterprise staff and management must be aware of security risks to enterprise resources from distributed threats, as well as options for protection, response, and recovery. IT staff must possess the skills to implement the selected options for mitigation and prevention. Organizational procurement policies must ensure that security lifecycle issues figure prominently in procurement decisions, to prevent insecure products from being added to or remaining connected to the system. These changes must occur in enterprises globally, rather than just domestically, to have a significant impact on the ecosystem.

Edge Devices: Current State

Devices are a diverse and growing technical domain of the ecosystem.[33] The Internet simultaneously supports multi-user computing systems, personal computing and mobile devices, operational technology (*e.g.*, supervisory control and data acquisition [SCADA] systems in industrial or manufacturing settings), and IoT devices across the ecosystem. As a general rule, edge devices play two diametrically opposed roles with respect to distributed threats: malicious actors compromise edge devices to create distributed threats, and edge devices may also be the target of the threat (*e.g.*, ransomware attacks distributed by botnets). Poorly secured endpoints can be both the sources and victims of attacks.

Malicious actors are motivated to construct botnets as cheaply and efficiently as possible. Over the years, the targets have evolved, ranging from business machines, to poorly secured home devices, to vulnerable systems run by hosting providers and cloud service providers, and, more recently, to IoT devices. These shifts in targeting reflect the promise and challenges offered by this technical domain with respect to creating a more resilient ecosystem. Personal computers and mobile devices are more secure than in years past. Meanwhile, connected devices have reached a level of sophistication and density that facilitates their targeting by automated code, while the benefits of modern security tools are lacking in those devices.

Edge devices may be vulnerable to compromise for a variety of reasons:

- Often, devices were not designed with security in mind. Developers are either unaware of good security design practices, assume that the device will be inaccessible (*e.g.*, on a local network inaccessible from the Internet), or want to avoid security solutions that impose additional cost, increase time to market, or make a device harder for consumers to use. The resulting design choices, such as hard-coded administrative passwords, create inherently insecure devices. In other cases, appropriate security controls are present but usability and user interfaces result in less-secure configurations.

[33] Gartner, *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*, (Feb. 7, 2017), *available at*: https://www.gartner.com/newsroom/id/3598917.

- Common software development techniques result in, optimistically, a flaw every 2,000 lines of code[34]—or more by many other metrics.[35] Many of these bugs create exploitable security vulnerabilities, such as buffer overflows.
- When bugs are discovered after products are deployed, products may be difficult or impossible to patch. These vulnerabilities are often far easier to exploit than to correct.
- Systems shipped with inappropriate default configuration settings, such as hard-coded passwords, are more vulnerable in operation.
- Systems may also be vulnerable because support is unavailable. This is often the case for old devices.
- The scale and diversity of deployed devices make easy fixes difficult and provide additional attack surfaces for malicious activity.

A number of major software developers have taken these lessons to heart and have established best current practices that can significantly reduce vulnerabilities of edge devices. For example, Microsoft's Software Development Life Cycle, or SDLC, ensures that security is considered from the beginning. Secure software development tools, such as input fuzzing[36] or static analysis,[37] reduce the number of vulnerabilities in software. Secure update services can correct vulnerabilities after discovery.[38] Systems are shipped in more secure configurations, so default settings need not be changed. As a result, modern servers, desktops, laptops, and smart phones offer significantly fewer opportunities for compromise. This translates to the cloud environment as well, with more-secure edge devices becoming a practical possibility. Hardware roots of trust, which demonstrate that systems have not been tampered with, are another innovation appearing in modern systems.

Unfortunately, IoT devices are often sorely lacking in security-focused features. These systems now offer the most attractive target to malicious actors, and are an increasingly large percentage of the devices in the ecosystem. In fact, the November 2016 Ericsson Mobility Report predicted that IoT devices will surpass mobile phones as the largest category of connected devices in 2018.[39] Given the level of security on IoT devices, that is a daunting prediction.

---

[34] *See Coverity Scan: Open Source Report 2014*, Synopsys, page 4, (2015), http://go.coverity.com/rs/157-LQW-289/images/2014-Coverity-Scan-Report.pdf.

[35] *See, e.g.*, Steve McConnell, *Code Complete: A Practical Handbook of Software Construction*, pages 521, 652, (Microsoft Press, 2nd ed. 2004), ISBN: 0735619670.

[36] "Fuzz testing (fuzzing) is a quality assurance technique used to discover coding errors and security loopholes in software, operating systems or networks. It involves inputting massive amounts of random data, called fuzz, to the test subject in an attempt to make it crash." TechTarget – SearchSecurity.com, definition of fuzz testing (fuzzing), https://searchsecurity.techtarget.com/definition/fuzz-testing (last updated Mar. 2010).

[37] "Static analysis, also called static code analysis, is a method of computer program debugging that is done by examining the code without executing the program." TechTarget – SearchWinDevelopment.com, definition of static analysis (static code analysis), https://searchwindevelopment.techtarget.com/definition/static-analysis (last updated Nov. 2006).

[38] The Software Assurance Forum for Excellence in Code (SAFECode), an industry consortium, has released a report to codify these lessons and offer further guidance on the SDLC model. Mark Belk et al., *Fundamental Practices for Secure Software Development: A Guide to the Most Effective Secure Development Practices in Use Today*, SAFECode, (2nd ed.) (Feb. 8, 2011), *available at* https://www.safecode.org/wp-content/uploads/2014/09/SAFECode_Dev_Practices0211.pdf.

[39] Ericsson, *Ericsson Mobility Report: On the Pulse of the Networked Society*, (Nov. 2016), https://www.ericsson.com/assets/local/mobility-report/documents/2016/ericsson-mobility-report-november-2016.pdf.

In addition, this domain of the ecosystem is not composed solely of modern devices. There are many legacy servers, desktops, laptops, and mobile phones in use today, and this will be the case for the foreseeable future. Legacy devices are no longer supported by their manufacturers, so their vulnerabilities cannot be easily addressed.[40] To make matters worse, attack tools for these devices or their vulnerable code components remain widely available.

Finally, high percentages of personal computing systems on the Internet run pirated software; one industry association's statistics for 2015 ranged from 17% in the U.S. to 70% in China and 84% in Indonesia.[41] Manufacturers typically restrict the distribution of security patches only to systems running legally purchased software, so these systems cannot be secured against known vulnerabilities. While vendors cannot reasonably be expected to provide support for unlicensed software, these unprotected systems provide another class of easy targets for malicious actors, and underscores the international nature of this challenge.

Insecure devices are not typically a result of limitations in the underlying technology. While imperfect, when applied properly, the current best practices are fairly effective, result in devices that are reasonably secure upon delivery, and include tools to maintain that level of security throughout the device's lifecycle. Commercial sectors that have embraced these practices, such as operating system developers, have demonstrated significant improvements in security and resilience.[42] Unfortunately, these security practices are implemented inconsistently. Many products are shipped with known bugs, do not include an update mechanism, and/or do not follow best current practices for administrative access.

Some of this challenge can be addressed with increased awareness and education. Some product developers do not understand how to leverage currently available tools for secure product development. Operational technology product developers understand their product line (*e.g.*, refrigerators) but may not understand basic security requirements for their products' network connectivity. Enterprise customers make procurement decisions without considering full lifecycle costs, as well as externalities of having an insecure network. End consumers may lack the tools to understand how certain product features protect them from security risks or how their devices may negatively impact the ecosystem.

Market incentives appear to exacerbate the problem. Product developers prioritize time to market and innovative functionality over security and resilience. Security features are not easily understood or communicated to the consumer, which makes it difficult to generate demand.

---

[40] For example, Microsoft discontinued support for twelve-year old Windows XP in April 2014. Two years later, between 7.4 and 10.9% of all desktops were still running XP and were described as "sitting ducks for cybercriminals to attack." John Zorabedian, *Millions of People Are Still Running Windows XP*, Naked Security (Apr. 11, 2016), https://nakedsecurity.sophos.com/2016/04/11/millions-of-people-are-still-running-windows-xp/.

[41] *See* BSA | The Software Alliance, *Seizing Opportunity Through License Compliance: BSA Global Software Survey*, (May 2016), http://www.bsa.org/~/media/Files/StudiesDownload/BSA_GSS_US.pdf.

[42] *See* Steven J. Vaughan-Nichols, *Security 2014: The Holes Are in the Apps, not the Operating Systems*, ZDNet (Feb. 28, 2014, 19:46 GMT), http://www.zdnet.com/article/security-2014-the-holes-are-in-the-apps-not-the-operating-systems/.

Vision for the Future of Edge Devices

Broad advances in the edge device technical domain are both possible and essential if we are to build a more resilient Internet and communications ecosystem. To be effective, these advances must be global, since the majority of Internet devices are located outside the United States. This global action will require globally accepted security standards and practices to be robust, widely understood, and applied ubiquitously. Those standards should be flexible, appropriately timed, open, voluntary, and industry-driven.

Devices must be able to resist attacks throughout their deployment lifecycles—at the time of shipment, during use, and through to end-of-life. For this to occur, security must become a primary design requirement. Vendors must not ship devices with known serious security flaws, must include a secure update mechanism, and must follow best current practices (*e.g.*, no hard-coded passwords, disabling software features that are not critical to operation) for system configuration and administration. Vendors should disclose the minimum duration of support to customers, and device manufacturers should maintain secure update services for the promised duration.[43]

Hardware roots of trust and trusted execution technologies are now a component of many off-the-shelf computing platforms. Future products will need to leverage these technologies to demonstrate authenticity and integrity at initial deployment and throughout the period of use. Modern development techniques rely on a combination of open source and commercially available components. To meet future security demands, such components must be traceable through the supply chain and offer greater assurance.

Such advances will require significant steps forward in awareness and education for product developers. All product developers must be equipped with the knowledge and skills required to apply the available tools for secure product development. The tool kits and components used by these vendors must reflect security concerns to achieve scale and keep pace with a changing developer workforce, and the partnerships and consortia driving standardized technology must empower developers to make and communicate security decisions. Meanwhile, operational-technology product developers must add basic security requirements to their product-specific knowledge and skills. At the same time, customers must be equipped with sufficient knowledge and information to select products designed to be secure in their environments, and must be aware of the risks presented by all devices, including legacy devices.

Lastly, market incentives will need to align with these security advances, so that product developers who prioritize security and resilience equally with time to market and innovative functionality are rewarded. Clear signals regarding product security and resilience that are accessible to customers will help improve these incentives. However, the value proposition for better security will likely start in the enterprise environment due to its economies of scale; once there is a generally accepted security posture in a given product class, few manufacturers would be likely to ignore it.

---

[43] *See*, *e.g.*, NTIA's Multistakeholder Process on Internet of Things Security Upgradability and Patching – Communicating Upgradability and Improving Transparency Working Group, *Communicating IoT Device Security Update Capability to Improve Transparency for Consumers*, (July 14, 2017), https://www.ntia.doc.gov/files/ntia/publications/draft_communicating_iot_security_update_capability_-_jul_14_2017_-_ntia_multistakeholder_process.pdf (helping manufacturers share details about security updates with consumers, and giving consumers the tools to know what to look for).

Home and Small Business Networks: Current State

Home and small business networks are becoming increasingly complex. Traditional computing devices interact with the cloud and other service providers to support an ever-increasing array of business and personal applications. IoT devices are already proliferating in great numbers in consumers' homes, from home automation devices such as lights, garage door openers, and thermostats, to connected home appliances and personal health and fitness monitors. This proliferation is the case in small businesses as well, where entrepreneurs and managers may seek to gain the benefit of off-the-shelf technology but lack an administrator or concerted IT strategies or policies. By all estimations, the number of connected consumer devices is expected to grow.

Unfortunately, this area of growth is also an area in which security is seriously lacking. The vast majority of home and small business users are unaware of cybersecurity risks, and many do not take the most basic security measures when connecting devices to their networks. Security-relevant decisions may be reached without customer input or knowledge if the device is set up and configured by someone else on their behalf or if the device uses a network other than the consumer's own network (for example, a cell network). Meanwhile, threat information sharing is challenging for small businesses, which typically lack the resources of large organizations to receive and process threat information.

As in the areas detailed above, many tools generally exist to mitigate cybersecurity risk, but it is unrealistic to expect the general population to be able to navigate the complex security environment. Small businesses and consumers can be victims of DDoS attacks—often in exchange for ransom to make the attacks stop—as well as unwitting hosts for devices used in a botnet. Home network products are not typically designed in a way that would allow home users to easily segment networks or configure security policies. Many home users rely on legacy devices or unlicensed systems. Furthermore, when a home user's device does become part of a botnet, it is often difficult for the network provider to tell which device is transmitting, because the NAT function, which allows home users to share a single IPv4 address among numerous devices behind a home router, obscures which device is being exploited.[44]

In the home and small business market, most home devices are unmanaged and thus unlikely to be updated manually, if automatic update features are not available. Consumer devices often ship with outdated software containing known vulnerabilities or hard-coded administrative passwords. Typical users may not be able to determine if the device's software is updated or if it even has a mechanism for software updates—many consumer devices do not. The typical user may not even be aware of the importance of this aspect, and may not have any access to substantive information about the software on a given device.

Even if the home or small business network is well architected and has strong security controls, some of the supported devices are likely to be mobile, and may connect to multiple networks during a typical day. These networks may not be as well managed, and devices may be compromised during their time on the outside network. These devices present an additional cybersecurity risk, permitting introduction of malicious code while circumventing local controls.

Generally, home and small business users do not have easy access to the information they need to select secure products, and they typically do not have tools to manage the products they have. While

[44] We also note that NAT technology offers some security benefits by limiting inbound traffic access to specific endpoints. This impedes (but does not completely eliminate) the threat from automated scanning and infection tools.

enterprise gateways are more likely to provide integrated security offerings, home users are unlikely to have access to the same level of service, and for those who do, many are not aware of the security offerings or the reason those services should be implemented. Fundamental security steps, such as changing a device's password from the default password or enabling secure encryption, are often beyond consumers' awareness or capabilities. In some instances, poor implementation of such requirements can frustrate users' efforts to implement these basic practices.

There is concern that consumers will not pay more for devices with better security.[45] The reality is that usually consumers' experiences are not directly affected by compromises of their devices; in fact, the consumer may never know that the device is part of a botnet. From the consumer's perspective, the webcam is still streaming, or the refrigerator is still chilling. For this reason, it may be challenging to hold owners responsible if their devices are used in a botnet. This lack of clear consequences of infection creates a challenge in motivating consumers to take steps to improve security—for example, to update those devices that are updateable.

Vision for the Future of Home and Small Business Networks

It is unrealistic to expect home users and small business proprietors to become security experts. However, there are steps industry stakeholders and others can take to improve the situation. In addition to awareness and education efforts to change consumer behavior, another approach is to engineer devices with users' behavior in mind. Ideally, devices marketed toward consumers should be designed with security built in. Consumer products should be designed as securely as possible, should include secure automated update mechanisms, and should have few to no requirements for managing the products.

Ideally, consumers will have access to commercial offerings that implement current best security practices, and will be able to easily recognize those offerings. Small business owners will similarly be able to map their purchases to their unique security concerns and obligations. They will be aware of the various risks related to unsecure IoT devices, and they will choose devices that are more secure. Nonprofits and commercial entities have begun evaluating products for privacy and data security;[46] efforts like these will raise awareness, and as awareness increases, so should device makers' interest in secure development. Over time, it should become easier and cheaper for manufacturers and integrators to adopt a secure development lifecycle.

While home users may not be especially motivated by fear that their devices could be used in a botnet, they may feel more compelled by concerns that their privacy, data, or access to services could be compromised. Many connected devices use cloud services for management and information storage, which has additional security and privacy implications. Fortunately, many of the same steps they would take to improve their privacy or data security and ensure uninterrupted access to services would also mitigate the chance of their devices becoming part of a botnet.

With properly applied incentives, market forces can play a key role in improved device security. For consumers to widely adopt more secure devices, the secure devices cannot cost significantly more than

[45] Bruce Schneier, *Security Economics of the Internet of Things*, Schneier on Security (Oct. 10, 2016, 10:26 AM) https://www.schneier.com/blog/archives/2016/10/security_econom_1.html (last updated Oct. 17, 2016).
[46] Consumer Reports, *Consumer Reports to Begin Evaluating Products, Services for Privacy and Data Security*, (Mar. 6, 2017), *available at* https://www.consumerreports.org/privacy/consumer-reports-to-begin-evaluating-products-services-for-privacy-and-data-security/.

insecure devices. Consumer products and services should be engineered with basic privacy and security protections built in. Buying guides that are easy to comprehend and provide actionable recommendations, targeted at specific home and small business needs, can generate the necessary market signals to reward developers and vendors for investing in security.

Smart routers and firewalls should be widely used to mitigate attacks and detect when a device has been compromised. As more home users' IoT devices transition to publicly addressable IPv6 addresses, ISPs will find it easier to identify end devices transmitting malicious traffic. Home users' networks enforce virtual network segmentation. Limiting devices' capabilities based on their intended uses—for example, limiting a connected toaster's activities on the network to solely those activities required to perform its toasting duties—would significantly limit the ability of botnets to capture home devices. A global decline in the home use of legacy products and pirated software would also vastly limit botnet perpetrators' opportunities.

Home users should be able to identify devices on their networks that increase their cybersecurity risk. Research and development is occurring to help security-conscious consumers better manage their networks. In 2017, the Federal Trade Commission's (FTC) IoT Home Inspector Challenge awarded its top prize to a proposal for a mobile app-based tool that would help users manage the IoT devices in their homes. The app would flag devices with out-of-date software and other common vulnerabilities and provide instructions on how to update each device's software and fix other vulnerabilities.[47]

Consumer education will need to become more effective, even if devices are better engineered to consumers' expected skill level. Meanwhile, an opportunity exists for a new workforce to support consumers' and small businesses' networking needs; this role could become a new vocation, more akin to electricians than electrical engineers, with appropriate training. The network and device industries can also make support easier and cheaper through standardization and coordination.

Governance, Policy, and Coordination

Because automated, distributed attacks on the global Internet are an ecosystem-wide problem, the issue will require coordination on policy and governance solutions across sectors. No single actor or sector is responsible for single-handedly addressing these risks, and no single entity can argue that these risks are all someone else's problem. For example, while many solutions involve active coordination with ISPs, putting sole responsibility at the network level would unwisely make all traffic dependent on this connective layer to determine what "good" traffic looks like, obligating ISPs to decide what fundamentally is and is not allowed on the Internet. Moreover, such ISP decision making would invariably both block traffic that in fact is "good," and miss traffic that should be blocked; encrypted traffic would exacerbate the problem.

Given the networked nature of the risks, real coordination is necessary to fully understand the problem and identify paths to solutions. While the information technology and communications sectors do actively work to understand security risks, some sectors find it challenging to share information and coordinate outside of their own sectors. Some entities coordinate domestically or regionally, but more sharing of information about threats, solutions, and their adoption and efficacy is needed worldwide. In

[47] Federal Trade Commission, *IoT Home Inspector Challenge*, https://www.ftc.gov/iot-home-inspector-challenge (last visited Apr. 4, 2018).

many cases, lack of clarity around roles and responsibilities has impeded collective action, resulting in security failures.

Some governments rely on overly specific regulations that quickly become obsolete, hinder innovation, and limit consumer benefit from dynamic sectors. Compliance requirements, or mandating specific regulations, may address some risks, but they can carry with them a greater burden while still leaving the broader ecosystem insecure or sending the signal that complying with the regulation is sufficient rather than the minimum necessary. The regulatory picture is further complicated by state or local regulation of edge devices, operational technology, and infrastructure. Solutions specific to particular countries or jurisdictions put at risk the global nature of an ecosystem where both bits and products flow with relative ease, and can put local innovators at a disadvantage.

This problem is further compounded by the cross-domain nature of networked technology. Lines have blurred among consumer technology, enterprise-grade tools and devices on which organizations depend, and safety-critical technology on which lives can depend. The same hardware and software can be used across the entire ecosystem. Key infrastructure services can be used by both a video game network and a company's corporate network.

In the law enforcement area, industry cooperation in taking down botnets is improving, but is not yet commonplace. Recent successful botnet takedowns involved extensive collaboration with industry in the cases of, for example, Kelihos, Gameover Zeus, and Coreflood. Active collaboration between law enforcement and the private sector has enabled disruption through seizures of key command and control assets. In the United States, in 2016, Federal Rule of Criminal Procedure 41(b)(6) was amended to address the unique challenges in investigating botnet activity, clarifying that courts may issue warrants authorizing the search of multiple computers when the identified computers are located in multiple judicial districts. In addition, federal law enforcement's ability to obtain civil injunctions—which has been indispensable in past botnet takedowns—is limited to cases that include elements of wiretapping or certain types of fraud. Taking down botnets in a safe, secure manner is a labor-intensive and lengthy process. In addition, law enforcement faces challenges with identifying and prosecuting malicious actors responsible for botnets, particularly those who operate outside the United States.

Vision for the Future of Governance, Policy, and Coordination

In the future, purchasers—whether end consumers or sophisticated enterprises—should be better able to understand the risks and security properties of connected devices. Approaches to IoT and computing devices are needed that will help not only promote consumer awareness, but will also drive the market, increasing the general adoption and use of better cybersecurity practices by device makers. That said, security risk evolves quickly; that which is deemed secure today may not be secure tomorrow, and is unlikely to be secure a decade from now. Market transparency solutions can empower buyers to make good decisions, but must also build in the context and timescale of the product lifecycle. Institutions that have relied on approaches that traditionally reflected static risk, such as purchasing requirements or insurance, will adapt to reflect the evolving nature of cybersecurity risk. Improved transparency about the software and hardware components of systems will help, as will appropriate incentives to understand the relevant risks for a given context and for the ecosystem as a whole.

Infrastructure players will better share and analyze data to foster a shared awareness of reputations across the ecosystem, and evaluate how well network partners are addressing risks in an evolving, efficient, decentralized manner. Mechanisms for information sharing should build on existing

multistakeholder mechanisms and communities, creating new opportunities to engage locally and globally.

As distributed threats evolve, new standards, guidelines, and metrics may be required to answer such new and emerging questions as: How can third parties best evaluate products for consumer benefits in a manner that is agile enough to keep up with quickly evolving security practices? What metrics and visibility into network management practices can inform us about infrastructure investment? More formalized but adaptable security expectations will allow us to introduce some accountability into security practices. Mechanisms such as voluntary frameworks can help both to shape incentives that motivate more secure design, and to create some accountability for failure to consider security and invest in secure devices. Any accountability mechanisms should reward those who make good risk-based decisions, while acknowledging that there is no such thing as perfect security.

To address the range of threats, all stakeholders, domestic and international, must more fully address automated, distributed attacks. At its core, that involves reducing the number of unsecured devices with access to the Internet to keep botnets to a manageable size, and developing mechanisms to share information about compromised systems and emerging attack trends up and down the network stack to the party (or parties) in the best position to respond to the threat.

Because technology deployment is truly trans-national, and information flows across international borders, none of this can be accomplished without international collaboration. In the international realm, the U.S. government robustly advocates for industry-led approaches and voluntary, consensus-based standards. As the NSTAC report stated, solutions depend on both standards and innovation at the network and Internet infrastructure layer. While a variety of relevant standards, frameworks, and best practices exist, they are not fully leveraged worldwide.

Governments can constructively influence the development of more secure products by steps such as supporting open, voluntary, industry-driven standards, and by conducting their own technology and device procurement decisions in a way that creates market incentives for more secure products. Security can also be promoted by increased multistakeholder engagement between the anti-abuse and global network infrastructure communities, as well as between cybersecurity and operational technology elements of industries that have not traditionally been focused on IT (*e.g.*, utilities or medical devices). For example, operational and multistakeholder engagement related to the Internet resources used by botnet managers for command and control is critical to threat signaling for network management and botnet detection. The United States should increase its international engagement in this area, particularly with countries that are already active on this issue.

Additionally, industry and law enforcement should work to find ways to coordinate more often and earlier to detect and prevent threat activity, and in managing incidents that take place. New tools and processes may improve information sharing among international law enforcement agencies. Law enforcement and industry groups should more effectively communicate on what is needed to successfully disrupt malicious networks and prosecute the actors behind it, while keeping privacy concerns in mind. Data-protection policies, both in the United States and internationally, should not disrupt existing tools, such as the widely used WHOIS database of domain ownership data.

Legal Landscape

Some stakeholders stressed the importance of minimizing uncertainty and legal risk to encourage private-sector collaboration with law enforcement agencies, more information sharing, vulnerability disclosure, and the ability to conduct effective countermeasures. Many also emphasized the need to harmonize legal approaches across sectors to avoid a patchwork of laws that could impede the IoT market.

Efforts are already underway to improve public-private relationships. DHS's National Cybersecurity and Communications Integration Center (NCCIC) serves as a central location where a diverse set of private sector and government partners involved in cybersecurity coordinate their efforts,[48] including information sharing, collaboration, and technical assistance.[49] Federal law already includes a structure for addressing some of the uncertainty and legal risk. The Cybersecurity Information Sharing Act of 2015 (CISA), for example, grants liability protection and other legal protections—such as antitrust protections, exceptions from disclosure laws and certain regulatory uses, and protections from privilege waivers—to private entities that share cyber threat indicators and defensive measures in compliance with the Act.[50] CISA designates the NCCIC as a central hub for the sharing of cyber threat indicators and defensive measures with the federal government.[51] These NCCIC cybersecurity capabilities and CISA legal protections apply to IoT cybersecurity in much the same way that they apply to cybersecurity more broadly. Moreover, nothing in CISA precludes robust sharing by private entities with law enforcement as part of the normal course of a criminal investigation; indeed, CISA authorizes the sharing of cyber threat indicators and defensive measures with law enforcement—or any other federal entity—and, in addition, its liability protection applies when such information is shared with law enforcement under certain circumstances.

Many stakeholders also stressed the importance of market incentives for securing IoT devices. Some touched on whether a liability regime informed by common best practices and standards might improve accountability in IoT device security. While this report does not engage in a comprehensive analysis of liability related to IoT device security, we expect this issue will continue to garner interest as the use of connected devices—devices that can impact the physical world—grows and questions regarding harms, privacy issues, consumer protection, causal chains, risk management, and possible state and court actions emerge. Liability is a complex area of law, as is the emerging IoT market, and care must be taken to avoid static and ineffectual compliance requirements, especially in the midst of a dynamic cybersecurity landscape. Investment must be made to address risk through innovative practices, and with stakeholders engaged in cross-sector coordination. Pressure to directly address this issue will grow if legal uncertainty is endemic and persistent.

Some stakeholders noted that any new legal or regulatory regimes may have unintended negative impacts on the IT industry if clear guidance is not included regarding what a vendor can do to limit its exposure. However, advocates caution against blanket liability protections without clear social gains from improved security processes. Some stakeholders, including civil society organizations, called for additional clarity regarding how existing laws in various jurisdictions apply in this area, how these laws can or should affect different stakeholders along the supply and distribution chains, and how to properly address harms. As this area continues to evolve, it is vital that the federal government better understand the interaction between liability and market incentives, as well as how any proposed changes might alter that dynamic. Care must be taken to ensure that our liability laws benefit consumers, protect stakeholders when appropriate, and avoid chilling innovation in today's digital environment. As public-private sector collaboration in this area continues, the federal government

should continue to monitor whether protection from liability related to information sharing is sufficient in today's environment to effectively address ongoing and new threats.

III. Goals and Actions

These goals and actions aim to present a portfolio of mutually supportive actions that, if implemented, would dramatically improve the resilience of the ecosystem. The recommended actions include ongoing activities that should be continued or expanded, as well as new initiatives. No single investment or activity can mitigate all threats, but organized discussions and stakeholder feedback will allow us to further evaluate and prioritize these activities based on their expected return on investment and ability to measurably impact ecosystem resilience. We look to stakeholders across the ecosystem to work with government to implement the proposed activities, realize opportunities for support and leadership, and remove impediments to implementation.

Goal 1: Identify a clear pathway toward an adaptable, sustainable, and secure technology marketplace.

To enhance the resilience of the Internet and communications ecosystem, it is critical that our technology marketplace support and reward the continuous development, adoption, and evolution of innovative security technologies and processes. When market incentives encourage manufacturers to feature security innovations as a balanced complement to functionality and performance, it increases adoption of tools and processes that result in more secure products. As these security features become more popular, increased demand will drive further research. As such tools are refined, it becomes cheaper for manufacturers, integrators, and system owner/operators to adopt the components of a secure development lifecycle, encouraging more manufacturers to differentiate their products based on the quality of their security features and thus enable greater competition. This section identifies actions that key stakeholders can take to establish an adaptable, sustainable, and secure technology marketplace.

Action 1.1 Using industry-led inclusive processes, establish internationally applicable IoT capability baselines supporting lifecycle security for home and industrial applications founded on voluntary, industry-driven international standards.

[48] *See* 6 U.S.C. § 148.
[49] *Id.* § 148(c).
[50] *See* Consolidated Appropriations Act, 2016, Division N – Cybersecurity Act of 2015 (Pub. L. No. 114-113, 129 Stat. 2242) (codified at 6 U.S.C. §§ 1501-1510).
[51] CISA provides an array of legal protections for cyber threat indicators and defensive measures that are shared with a federal entity in accordance with the statute. For instance, it provides protection from antitrust liability (6 U.S.C. § 1503(e)); federal and state disclosure laws (6 U.S.C. §§ 1504(d)(3) and 1503(d)(4)(B)); waiver of privileges (6 U.S.C. § 1504(d)(1)); and federal and state regulatory use (6 U.S.C. §§ 1503(d)(4)(C) and 1504(d)(5)(D)). When cyber threat indicators and defensive measures are shared with the NCCIC through the federal government's capability and process operated by DHS, such sharing also receives additional liability protections. 6 U.S.C. § 1504(c)(1)(B). Those additional liability protections are also available for sharing with other federal entities under limited circumstances. *See* 6 U.S.C. § 1504(c)(1)(B)(i) and (ii).

Security standards, baselines, and best practices have evolved over time for traditional computing devices, increasing the cost of assembling botnets with these devices. Rapidly increasing deployment of insecure IoT devices has had the pernicious side effect of enabling cost-effective development of extremely large and widely distributed botnets. For example, the Mirai botnets have compromised hundreds of thousands of devices as a result of hard-coded administrative passwords. More recently, the Reaper botnet has compromised devices by targeting well-known software vulnerabilities. While mitigations exist, many affected devices are not patchable. Since the passwords cannot be changed and the vulnerabilities cannot be patched, these devices will remain vulnerable throughout their lifecycle. These vulnerabilities could be mitigated in future IoT systems if the best current security practices for traditional computing devices, such as secure default configurations and effective software update mechanisms, were applied to IoT devices.

The impact of past botnets has been mitigated by actions taken by infrastructure providers such as ISPs—mainly cease and desist actions and absorbing excess traffic—but past mitigations were mainly reactive in nature, and the exponential increase in IoT devices and systems indicates diminishing returns for these traditional mitigation strategies. The ecosystem must become more resilient to distributed threats, starting with a proactive and focused approach on reducing known vulnerabilities of Internet-connected devices throughout the lifecycle.

Performance-based security capability baselines—which identify suites of voluntary standards, specifications, and security mechanisms that represent the combination of best practices for lifecycle security for a particular threat environment—are needed to accelerate the development and deployment of IoT devices and systems that are less vulnerable to compromise throughout their lifecycles.[52] For example, a baseline for home environments might include secure update mechanisms, such as automatic application of security patches and secure-by-default configurations, that minimize the need for user action. A security baseline for an industry might assume a dedicated and knowledgeable security staff that uses processes such as centrally managed updates. These baselines must be sufficiently flexible to apply where IoT devices are both a product and a service (*i.e.*, where cloud services are integral to product operation) and where security capabilities are distributed across a system of IoT devices.

When developing these baselines, we must balance the investment in baseline requirements against the costs of not using the baselines (*i.e.*, costs to those potentially harmed, cost to the product producer, and costs to other stakeholders). Capability baselines must be pragmatic to ensure that manufacturers can meet the requirements in a cost-effective manner, while offering a clear benefit to the customer and to the ecosystem. To achieve this balance, these baselines should be developed with industry leadership in collaboration with the intended customer (*e.g.*, a consortium representing an industrial sector, or consumer advocacy and civil society groups representing home users) and with active contribution and participation of governments as appropriate. Collaborative development of baselines provides manufacturers with lead-time and early insight into customer expectations, and increases the probability that conforming products will be available in a timely manner. Customer participation in baseline development may also provide a signal to the market that buyers prefer IoT devices that are designed to be secure in their target environments and also allow alignment of education activities described below. As the capabilities specified in the baseline become the de facto standard, this will support a sustainable market for more secure devices.

[52] Performance-based standards describe *what* must be achieved, rather than *how* to achieve it, reducing or eliminating negative impacts on innovation.

To ensure that lost innovation opportunity costs do not overwhelm the value of the baseline, IoT security baselines that identify small numbers of flexible security capabilities should impose minimal constraints (if any) on design and implementation.[53] Specifying capabilities in terms of performance rather than design (*i.e.*, an outcomes-based rather than prescriptive approach) will help manage costs associated with corresponding assessment programs. As an added benefit of limiting the feature set, it also becomes more practical for common development platforms to incorporate those feature sets into IoT components, simplifying development of conforming products.

A Foundation for Future Baselines

Several specifications have been published recently and offer, at a minimum, a strong foundation for future IoT security capability baselines. These efforts range from high-level specifications to extremely detailed documents and target a range of application environments. Notable examples of high-level specifications focused on consumer grade devices, all released since June 2017, include the Online Trust Alliance's IoT Security Framework,[54] the Digital Standard (developed by a coalition including Consumer Reports, Ranking Digital Rights, and the Cyber Independent Testing Lab),[55] and *Secure by Design: Improving the cyber security of consumer Internet of Things*[56] from the UK's Department for Digital, Culture, Media & Sport. One example of a detailed baseline specification is the *Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures,*[57] released in November 2017 by the European Union Agency For Network And Information Security, which identifies 83 technical measures and good security practices applicable to IoT security. Another example is "Security Tenets for Life Critical Embedded Systems," which was developed by a cross-sector working group comprised of Defense Industrial Base and Information Technology Sector members.[58]

Action 1.2 The federal government should leverage industry-developed capability baselines, where appropriate, in establishing capability baselines for IoT devices in U.S. government environments to meet federal security requirements, promote adoption of industry-led baselines, and accelerate international standardization.

Action 1.1 focuses on industry-led development of capability baselines for IoT devices in different threat environments. This approach creates multiple challenges, ranging from the development of multiple competing profiles to the absence of any baseline for a critical environment. In addition, where industry-led efforts are domestically focused, there may be challenges to gaining international acceptance. The federal government can accelerate convergence where multiple baselines exist, jump-start new efforts

[53] For example, a baseline might specify a requirement for unattended patch management without specifying a pull or push model, whether patches should be encrypted, or the exact type of integrity protection applied to the patch.
[54] *See* Online Trust Alliance, *Internet of Things*, https://otalliance.org/initiatives/internet-things (last visited Apr. 4, 2018).
[55] The Digital Standard, *The Standard*, https://www.thedigitalstandard.org/the-standard (last visited Apr. 4, 2018).
[56] Department for Digital, Culture, Media & Sport, *Secure by Design: Improving the cyber security of consumer Internet of Things*, (Mar. 7, 2018), *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf.
[57] European Union Agency for Network and Information Security, *Baseline Security Recommendations for Internet of Things in the context of Critical Information Infrastructures*, (Nov. 20, 2017), *available at* https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.
[58] U.S. Department of Homeland Security, *Security Tenets for Life Critical Embedded Systems*, https://www.dhs.gov/publication/security-tenets-lces (last published Jan. 12, 2017).

by establishing a draft for discussion where no baseline exists, and encourage international standardization by establishing federal IoT baselines.

By establishing federal IoT security capability baselines in coordination with industry, civil society, and international partners, the federal government can demonstrate the practicality and efficacy of the specified capabilities, contribute to market incentives, and establish a basis for practical assessment programs (see Actions 5.1 and 5.2). This approach will also ensure that federal government baselines will reflect the state of the art and evolve as industry and market evolves. The National Institute of Standards and Technology (NIST) is responsible for developing information security standards and guidelines, including minimum requirements for federal systems. NIST should identify security requirements for IoT devices and systems in federal environments. Where industry-led consensus baselines exist, NIST should assess their applicability to federal security requirements and, if appropriate, develop a federal standard by reference. These federal capability baselines would be similar to (and track progression of) the industry-led baselines developed in Action 1.1. If an appropriate baseline is not available, NIST should seek industry partners for the development of a practical baseline and draft for discussion for future industry-led efforts.

As the efficacy of these baselines is proven, the U.S. government and industry should also jointly engage with developers of industry-led, voluntary international standards and specifications to establish globally relevant standards. As these standards and specifications emerge, federal baselines should be created, updated, or replaced as appropriate.

The venue for standardization of these baselines must be selected carefully. The security baselines and any supporting standards and specifications should be developed in private-sector bodies that are open to participation by all interested stakeholders, and should be developed in a transparent manner, using balanced consensus-based processes, and taking a results-based—rather than requirements-based—approach wherever possible. Such performance-based standards are best suited for addressing the challenges posed by a rapidly evolving technology space, such as IoT. These processes do not exclude government participation, but ensure that government, industry, civil society, and users' interests are all well represented, and that the resulting solutions reflect the state of the art in that technology space. The flexibility of these processes also enables standards to be updated as technology, threats, and solutions evolve. The strong alignment between businesses' use of standards that they helped develop and governments' support for the development of these tools facilitates adoption of these standards on a large scale.

It is important to recognize that, given the breadth of the technology space, no single standards or specification development organization can develop all the solutions. Governments around the world need to support cooperation and coordination between standards and specification bodies that have the expertise and experience, and develop products along the principles discussed above, to ensure robust, timely, and fit-for-purpose solutions. In the United States, NIST should continue to lead and coordinate federal agencies' engagement on related standards activities, including engagement with the private sector, exploring a federal government strategy in support of international standards to address the challenges of botnets and other automated, distributed threats.

Complementary actions by the U.S. government and private sector could significantly enhance the impacts of these federal IoT capability baselines. The federal government can use acquisition rules and procurement guidelines to amplify the market signal by requiring the capabilities in the baseline(s) (see

Action 2.3) and, if appropriate, preferring products that also conform with a given private-sector labeling scheme (see Actions 5.1 and 5.2).

Action 1.3 Software development tools and processes to significantly reduce the incidence of security vulnerabilities in commercial-off-the-shelf software must be more widely adopted by industry. The federal government should collaborate with industry to encourage further enhancement and application of these practices and to improve marketplace adoption and accountability.

Common software development techniques result in software with at least one bug per 2,000 lines of code,[59] and modern systems include tens of millions of lines of code. This implies tens of thousands of bugs in a system, many of which create security vulnerabilities. Secure update mechanisms (noted as an important baseline feature in Action 1.1) allow vendors to correct these errors after a relatively brief vulnerability period. However, avoiding such vulnerabilities altogether would have an even more significant impact in terms of reducing security risk. While it is possible to develop code with very small numbers of errors, where the importance of mission merits a significant reduction in productivity, the challenge is developing mechanisms that produce significantly better code without unduly reducing productivity.

An interagency task force (documented in NIST Interagency/Internal Report [NISTIR] 8151[60]) identified numerous approaches to developing software with fewer vulnerabilities, implementing three basic strategies:

- Stopping vulnerabilities before they occur, including improved methods for specifying and building software;
- Finding vulnerabilities, including better testing techniques and more efficient use of multiple testing methods; and
- Reducing the impact of vulnerabilities by building architectures that are more resilient, so that vulnerabilities cannot be meaningfully exploited.

Tools to support these approaches are available now,[61] and have been embraced by a few forward-leaning firms.[62] Software developers should begin transitioning to these tools immediately, focusing initially on the products that present the highest risk. DHS and the FTC offer resources for smaller software developers as well.[63]

---

[59] *See Coverity Scan*, *supra* note 34, at page 4.

[60] Paul E. Black, Lee Badger, Barbara Guttman & Elizabeth Fong, *Dramatically Reducing Software Vulnerabilities: Report to the White House Office of Science and Technology Policy*, (Nov. 2016), NIST Interagency/Internal Report No. 8151, *available at* http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8151.pdf.

[61] *See*, *e.g.*, *CWE/SANS Top 25 Most Dangerous Software Errors*, SANS Institute, https://www.sans.org/top25-software-errors/ (last updated June 27, 2011).

[62] For example, the Software Assurance Marketplace (SWAMP) aims to make it easier to consistently test the quality and security of these applications and bring a transformative change to the software assurance landscape by reducing the number of weaknesses deployed in software. For more information, see Software Assurance Marketplace, https://continuousassurance.org/ (last visited Apr. 4, 2018).

[63] DHS supported the development of the SWAMP, which offers both cloud-based and open source software assurance tools. For more information, see Software Assurance Marketplace, *About Swamp*, https://continuousassurance.org/about-us/ (last visited Apr. 4, 2018); Federal Trade Commission, *Careful Connections: Building Security in the Internet of Things*, (Jan. 2015),

The federal government should support industry adoption of these tools through efforts that improve return on investment or create market incentives for lagging sectors or industry groups, as the NSTAC also recommended in its report. The federal government should promote the further development of tools for secure coding practices by sponsoring or performing targeted research (see Action 1.4), and sponsoring competitions for secure toolchains (multi-tool processes for software development) to demonstrate their effectiveness and productivity. The federal government should also work with industry and civil society to develop strategies that make it easier and cheaper to adopt these approaches—including education and training discussed in detail below—keeping in mind the requirements of small businesses, and work with the full range of stakeholders to make such a process observable and verifiable to third parties.

As an example, modern products use many software components, libraries, and modules, some of which may be outdated or vulnerable and are not always closely tracked by manufacturers in the rapid development cycle. While the notion of transparency around components of software is not new, wide support and adoption has not been realized. NTIA should engage diverse stakeholders in examining the strategies and policies necessary to foster a marketplace for greater software component transparency, including identifying and exploring market and other barriers that may inhibit progress in this space. Knowing what software has been incorporated into a product is a fundamental step toward being able to keep it updated and to mitigate threats when they arise.

Action 1.4 Industry should expedite the development and deployment of innovative technologies for prevention and mitigation of distributed threats. Accordingly, where relevant, government should prioritize the application of research and development funds and technology transition efforts to support advancements in DDoS prevention and mitigation, as well as foundational technologies to prevent botnet creation. Where appropriate, civil society should amplify those efforts.

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 (AI), is urgently needed to get ahead of malicious actors. Innovations will be needed to address other botnet-supported malicious activities, such as ransomware and computational propaganda. Foundational technologies to prevent, detect, and recover from compromise and incorporation into a botnet will be required to address these and future attacks.

To enhance the resilience of the ecosystem, successes in research and development must be capitalized upon through aggressive deployment. Innovative device technologies, such as hardware roots of trust or enhanced device authentication mechanisms, offer the potential for significantly stronger security throughout the product lifecycle. Advances in network tools, such as the Manufacturer's Usage Description (MUD), a standard currently under development in the IETF,[64] could enhance the resilience of the network by managing communications for security and making granular network management

https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf.

[64] *See* E. Lear, R. Droms & D. Romascanu, *Manufacturer Usage Description Specification* (Draft), Internet Engineering Task Force – Network Working Group, https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/ (last updated Apr. 19, 2018).

cheaper and easier. Accelerated adoption of such innovative technologies would improve the resilience of the ecosystem, but commercialization and adoption of promising research results to create viable products or marketable services is notoriously challenging. Civil society and nonprofit groups can also amplify new platforms or solutions, as the Internet Society and Global Cyber Alliance have done for their respective initiatives promoting routing security,[65,66] and the American Civil Liberties Union has done for its initiative on privacy and technology.[67]

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. Departments and agencies also sponsor applied research in support of mission requirements and a variety of technology transition activities.[68] Agencies should prioritize development and deployment of innovations that would increase the resilience of the ecosystem and coordinate these investments through the Networking and Information Technology Research and Development (NITRD) program.[69] As with the use of any mitigation techniques, steps should be taken to ensure that these innovative technologies do not open consumers to unnecessary privacy risk. This can be done through privacy risk assessment tools described in NISTIR 8062,[70] or through a Privacy Impact Assessment.[71]

Action 1.5 Government, industry, and civil society should collaborate to ensure that existing best practices, frameworks, and guidelines relevant to IoT, as well as procedures to ensure transparency, are more widely adopted across the digital ecosystem. Emerging risks in the IoT space must be addressed in an open and inclusive fashion.

Several previous efforts have produced guidance and best practices related to botnets and better IoT security, but botnets remain a problem. For example, the stakeholders in NTIA's multistakeholder process on IoT Security Upgradability and Patching developed a set of documents offering solutions to both the supply and demand side of the IoT consumer market, but stakeholders also emphasized the shared role in promoting these ideas across the IoT community.[72] Publishing documents is not enough—we must work to ensure they are widely adopted across the ecosystem. The IoT community must work collaboratively to identify and adopt existing best practices, frameworks, and guidelines that are

[65] *See* Internet Society, *MANRS: Mutually Agreed Norms for Routing Security*, https://www.internetsociety.org/issues/manrs/ (last visited Apr. 4, 2018).
[66] *See* Global Cyber Alliance, *Quad9: Four Simple Steps to Security*, *Privacy and Performance*, https://www.globalcyberalliance.org/initiatives/quad9.html (last visited Apr. 4, 2018).
[67] *See* ACLU, *Privacy & Technology*, https://www.aclu.org/issues/privacy-technology (last visited Apr. 4, 2018).
[68] DHS's Distributed Denial of Service Defense project is an example of such research. *See* U.S. Department of Homeland Security, *Distributed Denial of Service Defense*, https://www.dhs.gov/science-and-technology/csd-ddosd (last visited Apr. 4, 2018). *See also* National Science Foundation, *Secure and Trustworthy Cyberspace (SaTC)*, https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504709 (last visited Apr. 4, 2018).
[69] The Networking and Information Technology Research and Development Program, https://www.nitrd.gov/ (last visited Apr. 4, 2018).
[70] Sean Brooks, Michael Garcia, Naomi Lefkovitz, Suzanne Lightman & Ellen Nadeau, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, (Jan. 2017), NIST Interagency/Internal Report No. 8062, *available at* https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.
[71] For more information on one type of Privacy Impact Assessment, see U.S. Department of Homeland Security, *Privacy Impact Assessment Guidance*, https://www.dhs.gov/publication/privacy-impact-assessment-guidance (last published Apr. 13, 2018).
[72] NTIA Multistakeholder Process on Internet of Things Security Upgradability and Patching, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security (last updated Nov. 7, 2017).

relevant to IoT. The IoT community should also work to raise awareness of these best practices, frameworks, and guidelines. The NSTAC report also noted this need, related to its recommendation that industry should work with DHS and Commerce to accelerate adoption of security guidelines.

The federal government should support widespread adoption of best practices by engaging the community to determine why the prior recommendations were not widely implemented or were unsuccessful, identify appropriate paths for driving successful implementation, and focus on practical, proven tools and levers. For example, current development practices emphasize reuse of open source and commercial software, which may be outdated or vulnerable, but these attributes of (in)security are obscured from developers and customers alike. NTIA's multistakeholder process on software component transparency (see Action 1.3) can explore how to increase assurances that no known vulnerabilities are shipped with products.

One particularly vexing problem that will require stakeholder input is the question of legacy and orphan code, or "dead software." Stakeholders in NTIA's patching multistakeholder process identified the importance of communicating the period for which security updates would be provided, but did not offer explicit guidance as to what would happen when security updates are no longer offered.[73] As durable goods with long life spans are increasingly connected with fragile code, this problem will grow. One security expert even went so far as to advocate that abandoned software be made open source.[74] Access to the code is only one obstacle, however. Updates must still be written and tested. Bankrupt vendors present further challenges if signing certificates or MUD files (see Action 1.4) are tied to domains. One model for addressing the externalities of insufficiently supported software comes from the Core Infrastructure Initiative,[75] but the prospect of systematically coping with globally distributed unmaintained systems will require input from a wide range of stakeholders.

Transparent and verifiable software asset management (SAM) practices can help enterprises to identify software that cannot be patched because updates are no longer available or licenses have expired. Once identified, enterprises can address these vulnerabilities by replacing products or re-architecting networks to manage risk. Enterprises and government stakeholders should adopt SAM practices based on international standards for procurement and asset management, as well as procedures for mitigating risks identified through these practices.

Complementary efforts to increase awareness and educate product developers and manufacturers could significantly enhance the impact of these best practices, frameworks, and guidelines, as described in Actions 5.3, 5.4, and 5.5.

[73] The FTC's report on mobile security updates recommends that companies consider disclosure of minimum support period and notifications before security support period ends. Federal Trade Commission, *Mobile Security Updates: Understanding the Issues*, (Feb. 2018), https://www.ftc.gov/system/files/documents/reports/mobile-security-updates-understanding-issues/mobile_security_updates_understanding_the_issues_publication_final.pdf.
[74] Dan Geer, Keynote Address at Black Hat USA 2014: *Cybersecurity as Realpolitik*, (Aug. 6, 2014), *available at* http://geer.tinho.net/geer.blackhat.6viii14.txt (nominal delivery draft). Video available at: https://www.blackhat.com/us-14/video/cybersecurity-as-realpolitik.html.
[75] Core Infrastructure Initiative, https://www.coreinfrastructure.org/ (last visited Apr. 4, 2018).

Goal 2: Promote innovation in the infrastructure for dynamic adaptation to evolving threats.

To establish a more resilient Internet and communications ecosystem, standards and practices that deter, prevent, and/or mitigate botnets and distributed threats should be continually implemented and upgraded in all domains of the ecosystem in response to and anticipation of the evolving threat. This section identifies actions available to stakeholders to support development of an effective and dynamic infrastructure.

Action 2.1 Internet service providers and their peering partners[76] should expand current information sharing to achieve more timely and effective sharing of actionable threat information both domestically and globally.

Once established, botnets are re-sold or rented to multiple customers and redirected to attack new targets. This means many ISPs and their peering partners will experience similar attacks over time. When an ISP first faces a particular threat, anomalous behavior must be analyzed and mitigation methods developed. Botnets are generally distributed across many ISPs, each of which can contribute to mitigation activities given sufficient knowledge. Sharing network management techniques and defensive tactics that are effective against particular threats is another way large network providers increase the preemptive value of the information shared.

Current information-sharing arrangements between ISPs and their peering partners are highly effective within their scopes. By sharing information about known, ongoing, and emerging threats, ISPs are able to respond more efficiently. However, current information-sharing arrangements are often driven by personal relationships and are not comprehensive, especially when dealing with more nuanced or sensitive threats. An evolving network landscape—and the changing scope, scale, focus, and diversity of network players—also impacts the effectiveness of sharing relationships. Collaboration between ISPs and their peering partners should be formalized and include sharing of detection, notification, and planned or utilized mitigation methods within the network. Where sharing is encumbered by commercial concerns, ISPs should seek ways to address sharing arrangements and response coordination in their peering and transit agreements.

Industry should lead efforts to expand the scope and utility of information sharing between ISPs and their peering partners and to address gaps in operationalizing the information shared. In particular, industry should work collaboratively with civil society and government to improve coordinated responses to actionable information and lead the development, refinement, and standardization of information-sharing protocols to increase speed and permit automated response. Special attention should be given to engagement and inclusion of smaller ISPs and protocol developments that enhance their participation.

While industry has the lead role, the federal government can facilitate this activity domestically through the Communications Information Sharing and Analysis Center (ISAC) (*i.e.*, the National Coordinating Center for Communications [NCC]), by forging partnerships with network operator groups (NOGs), internationally through continued engagement in the Forum of Incident Response and Security Teams (FIRST), and by expanding information-sharing agreements with international peers such as Telecom ISAC Japan. The government can play an important role in these discussions, convening

[76] This includes enterprises that operate their own BGP routers and DNS servers.

multistakeholder meetings where needed, providing a global view, and ensuring that the process is equitable for all stakeholders. National Computer Security Incident Response Teams (CSIRTs) can also coordinate directly, and can catalyze a response by local resource managers and infrastructure players.

Action 2.2 Stakeholders and subject matter experts, in consultation with NIST, should lead the development of a CSF Profile for Enterprise DDoS Prevention and Mitigation.

DDoS-aware enterprises that wish to mitigate the impact of future DDoS attacks and reduce the likelihood that internal resources are incorporated into botnets to attack other enterprises find that comprehensive guidelines are not readily available. Large enterprises are forced to devote significant staff resources to identifying and procuring or deploying appropriate mechanisms. Smaller businesses often lack the expertise or cannot afford to divert those resources to developing an anti-DDoS strategy. Comprehensive solutions are complex, and often require a combination of locally managed and external commercial services, so communicating needs to vendors is critical.

The Framework for Improving Critical Infrastructure Cybersecurity (known as the CSF) version 1.0 was developed by NIST with extensive private-sector input, as was version 1.1, released in April 2018. The CSF provides a flexible approach to managing cybersecurity risk that incorporates industry standards and best practices, is sufficiently general to allow for broad applicability in a variety of environments—including IoT—and has been widely accepted by industry. The CSF may be supplemented by Framework Profiles, which apply the Framework components to a specific situation. In particular, industry sectors can use profiles to document best practices for protection against specific threats. The CSF is designed to evolve over time as the cybersecurity environment changes.

Enterprises that wish to enhance the resilience of their own networks against DDoS attacks and protect against botnets incorporating their resources would significantly benefit from the availability of a CSF Profile[77] for Enterprise DDoS Prevention and Mitigation. An industry-led effort, in consultation with NIST, academia, and other subject matter experts, should develop a CSF Profile for Enterprise DDoS Prevention and Mitigation, focusing on the desired state of organizational cybersecurity to mitigate DDoS attacks.[78] The CSF Profile would provide guidance to enterprises and establish a common language for discussions regarding DDoS protection mechanisms with product vendors, ISPs, and other infrastructure providers. The profile would help enterprises identify opportunities to improve DDoS threat mitigation and aid in cybersecurity prioritization by comparing their current state with the desired target state. The profile would likely include multiple levels to support industry sectors with different resilience requirements.

The scope of the CSF Profile should include, at a minimum, on- and off-premise DDoS mitigation mechanisms, routing security features (*e.g.*, Best Current Practice [BCP] 38/84 ingress filtering), and guidance on closing reflection vectors. For broadest applicability, the Profile should be written to cover both large enterprises, which may operate key components of their DDoS mitigation strategies, and small businesses, which often rely entirely on service providers.

[77] CSF Profiles are compilations of guidance and best practices around particular threats that follow the well-established CSF model.

[78] The Coalition for Cybersecurity Policy & Law (Cybersecurity Coalition) has initiated a promising effort, currently in draft form. *See* Cybersecurity Coalition, *Threat Profile for DDoS Attacks Using NIST Framework*, https://www.cybersecuritycoalition.org/threat-profile-ddos-nist-framework (Jul. 28, 2017).

Government stakeholders should participate in the development to ensure the profile is broadly applicable enough to serve as a CSF Profile for Federal DDoS Prevention and Mitigation. To create market incentives, this action should be supported by aggressive adoption throughout the federal government as specified in Action 2.3, either through direct application of the profile or through application of corresponding controls using the existing Federal Information Security Modernization Act process.

Action 2.3 The federal government should lead by example and demonstrate practicality of technologies, creating market incentives for early adopters.

Upon publication of the device IoT security baselines (Action 1.1), the federal government should establish procurement guidelines to provide market incentives for early adopters. Many IoT product vendors have articulated plans to enhance the security of their products, but observers have expressed concern that market incentives are heavily weighted toward cost and time to market. Without evidence that customers will absorb the additional cost to develop more secure products, the industry may be incentivized toward a race to the bottom. While federal procurement no longer dominates the market, its buying power and influence is still strong, and the U.S. government can lead by example. By developing guidelines for federal procurement actions based on the security baselines for IoT devices, the U.S. government can establish market incentives for early adopters. The Office of Management and Budget, General Services Administration (GSA), and Department of Defense can facilitate these procurement requirements through policy and modifications to the GSA schedule and federal acquisition regulations.[79]

Upon publication of an appropriate CSF profile (Action 2.2), the federal government should implement basic DDoS prevention and mitigation measures for all federal networks to enhance the resilience of the ecosystem and demonstrate the practicality and efficacy of the profile. In the past, hackers have leveraged federal networks in DDoS attacks using open resolvers and other agency resources to amplify their attacks. The federal government should lead by example, ensuring that federal resources are not unwitting participants and that federal networks are prepared to detect, mitigate, and respond as necessary. The Administration should mandate implementation of the Federal CSF Profile for DDoS Prevention and Mitigation by all government agencies within a fixed period after completion and publication of the profile.

The federal government should evaluate and implement effective ways to incentivize the use of software development tools and processes that significantly reduce the incidence of security vulnerabilities in all federal software procurements, such as through attestation or certification requirements. To establish market incentives for secure software development, the federal government should establish procurement regulations that favor or require commercial-off-the-shelf software that is developed using such processes, when available. The federal government should also ensure that government-funded software development projects use the best available tools to obtain insight into the impact of these regulations.

[79] The DHS-led Information Technology Coordinating Council's IoT Security Working Group is currently drafting guidance for procurement officers on questions to ask their customers, their IT and security teams, and the vendors to ensure that a procured connected device fits into the agency's risk management posture. This guidance will complement, but is not the same as, compliance guidelines built in relation to security baselines.

Action 2.4 Industry, government, and civil society should collaborate with the full range of stakeholders to continue to enhance and standardize information-sharing protocols.

To address automated, distributed threats, stakeholders must share robust information in a near-real-time manner. As a key lesson learned, the NSTAC report indicated that collaboration between the public and private sectors is vital to mitigating botnets. Information-sharing protocols currently in use were pioneered by the federal government, with active input from a wide range of stakeholders, but may not meet the needs of all stakeholders.

For example, small businesses are underrepresented; they do not contribute to or benefit from most current information-sharing arrangements. To meet the needs of small businesses, which generally lack a robust in-house cybersecurity team, protocols may need to enable automated action. For example, ISPs can often identify the customer network associated with a compromised device, but lack the visibility to identify specific devices. Small businesses may not be able to identify these devices if contacted by their ISPs. Information-sharing protocols that permitted ISPs to share information about detected compromised devices with the routers supporting small businesses could permit automated identification and more robust customer control of their networked devices. Customers might also choose to share the results of any mitigation steps with their ISPs as well, similarly to sharing software failure information with vendors.

To meet the coordination and collaboration needs of a highly resilient infrastructure, these information-sharing protocols must be comprehensive in scope, accessible to a broad range of enterprises, and sufficiently precise to permit automated processing and response. To ensure that these goals are met, industry should lead efforts, in collaboration with the federal government and other stakeholders, to enhance information-sharing protocols to meet stakeholder needs and establish international standards to facilitate global coordination.

Action 2.5 The federal government should work with U.S. and global infrastructure providers to expand best practices on network traffic management across the ecosystem.

While network providers cannot be expected to serve as traffic cops and identify all bad packets, both common and newer tools and practices can help filter out some types of bad traffic. Many market actors use either informal reputation signaling or more formal peering and transit agreements to address traffic management. A broad coalition of domestic and international experts—industry, academia, civil society, and government—should examine the extent to which inter-autonomous system, internetwork peering, and transit agreements might improve traffic management accountability—for instance, as applied to anti-spoofing and filtering. The academic and engineering community should research how new tools and practices in development might also be incorporated and implemented. Industry, academia, civil society, and the federal government should build upon these findings to expand constructive policies and best practices on network traffic management across the ecosystem, keeping in mind the requirements of small business. Existing tools and frameworks, such as the U.S. Anti-Bot Code of Conduct for ISPs and the voluntary Mutually Agreed Norms for Routing Security (MANRS), should be reviewed, and new solutions should be explored in a multistakeholder process that includes a diverse representation of network players that map to today's ecosystem environment.

Goal 3: Promote innovation at the edge of the network to prevent, detect, and mitigate automated, distributed attacks.

To establish a resilient Internet and communications ecosystem, infrastructure services designed to protect against attacks should be complemented by increased detection and mitigation of compromised devices in home or enterprise networks, and where those networks connect to the Internet. More context from local knowledge can improve detection, and it may be easier to simply segment off or firewall particular devices or services behaving anomalously. This section identifies actions stakeholders can take to manage the impact of the compromised devices used in automated, distributed attacks.

Action 3.1 The networking industry should expand current product development and standardization efforts for effective and secure traffic management in home and enterprise environments.

The networking industry is pursuing a variety of proprietary and standards-based mechanisms to better manage traffic within enterprise networks. These mechanisms aim to prevent communications with suspicious systems or constrain communications to hosts specifically required for correct operations. These systems may leverage AI or machine learning, threat detection and mitigation methods provided by external commercial services, or device-specific information. Industry should expand these efforts to accelerate the delivery of efficient and cost-effective network security for both home and enterprise environments.

Local network hubs and gateways[80] can act as traffic managers, identifying and preventing malicious traffic from accessing IoT devices and limiting harmful traffic emanating from devices in the local network. Cloud providers are also developing solutions that might layer with these gateway-focused solutions, potentially providing multiple checks and balances in the network stack to better secure the IoT ecosystem. As these security innovations emerge, government and stakeholders should partner to increase awareness of security solutions among consumers, small and medium enterprises, and international partners. Where specific barriers to adoption or advancement exist, government and stakeholders should convene to identify obstacles, to promote deployment of emerging standards, and to examine practical firewall policies for the broader product space.

Action 3.2 Home IT and IoT products should be easy to understand and simple to use securely.

Home IT and IoT products should reduce or eliminate the knowledge required to use them securely and privately. Enterprise networks benefit from the attention of professional staff who are charged with maintaining the security of the network and systems. Such personnel are often aware of and sufficiently skilled to configure these devices to a secure baseline. The administrative interfaces for most IT and IoT devices are designed for personnel with this background and skill level.

The owners of home and small business networks are less likely to have such support, with the inevitable result of insecurely deployed networks and products. Rather than expect consumers to become security experts, the IT and IoT industries should prioritize simple and straightforward deployment and configuration processes for devices marketed to home and small businesses. For

[80] Gateways are network architecture components that sit between subcomponents of the network. *See supra* Section II for discussions around smart gateways, etc.

example, if the installation process does not force updates to administrative passwords, these products will continue to be easy targets for incorporation into botnets. Default configurations should be the most secure for the intended scope of use, and cloud or application-based interfaces should be intuitive and rely on best current design practices. Installing security patches should be automatic or very easy to manage (*e.g.*, should not require downloads to flash drives).

Action 3.3 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.

A variety of effective anti-DDoS products and services are currently available, and innovative new products (such as those described in Action 3.1) have recently emerged. However, most enterprises have architected their networks for simplicity and performance rather than security. In combination with the CSF Profile for DDoS Prevention and Mitigation, enterprises have an opportunity to re-architect their networks to isolate insecure devices, manage communication flows, and generally enhance the resilience of their areas of the ecosystem. For example, enterprises that depend upon legacy systems should architect their networks so that these insecure devices are not exposed to attacks from the general Internet.

The risks coming from enterprise networks goes beyond the danger of hijacked IoT devices. Some network-based services allow malicious actors to amplify an attack through "reflectors," or services that can send large amounts of traffic to a spoofed target. If misconfigured to allow queries from anywhere on the Internet, vulnerable services such as DNS servers allow attackers to send huge volumes of traffic against victims. In 2018, one of the largest DDoS attacks seen to date exploited a newly discovered vulnerability in the relatively obscure MemCacheD software.[81] These flaws are often more problematic because the vulnerable systems are on enterprise-scale machines and networks with high availability and high bandwidth. Organizations should follow best practices for Internet-facing tools, and ensure that they are up to date.

Some of this evolution toward better network practices may occur organically as enterprises integrate more IoT devices into their networked environments and become more aware of the risks of externally facing applications. However, government, industry, and civil society should work to improve user and enterprise knowledge of threats and best security practices through collaborations such as partnership campaigns and strategic engagement activities. As such knowledge is formalized, it could be considered for inclusion in future versions of the NIST Cybersecurity Framework.

Action 3.4 The federal government should investigate how wider IPv6 deployment can alter the economics of both attack and defense.

North America ran out of easily distributed unused IPv4 addresses in 2015, yet very few consumers and small businesses currently take advantage of IPv6 address space and capabilities. Government and industry have been planning and working for broader IPv6 adoption, but should also consider how this will change the potential attack space and magnitude of automated, distributed attacks.

[81] Lili Hay Newman, *GitHub Survived the Biggest DDoS Attack Ever Recorded*, Wired (Mar. 1, 2018, 11:01 AM), https://www.wired.com/story/github-ddos-memcached/.

One challenge around notifying consumers that a device on their network has been linked to malicious activity is the large number of devices typically connected to a home or small business network. NAT-enabled routers, which can make many devices appear as if they have the same IP address, can impede notification. As we transition to IPv6, consumer ISPs may be better positioned to observe device-specific misbehavior when IPv6 addresses are not subjected to NAT. This information can, in turn, map to other edge-focused solutions.

Implementing NAT-enabled routers at the consumer and small business level has at times served as a key protection of vulnerable endpoints. NAT tools act as an incidental firewall, preventing devices in the home from being directly reached by the sort of mass-scanning tools that spread malware and lead to widespread infection; security cameras were a common target in the Mirai botnet because they typically do not sit behind a NAT-enabled router. In current architectures, a network that is IPv6-based would likely allow each device to be addressable. In theory, the IPv6 address space is so large that it would not be scannable using existing tools, but experts have observed that patterns would allow new scanning techniques to still discover vulnerable devices.

NTIA should work with stakeholders to identify lessons learned from industry and other countries, further examining impediments and options to align incentives to encourage ISPs to fully transition to IPv6 more quickly. Enabling the defense and mitigating the risk will require further innovation at the edge of the network. Understanding this sooner will provide for better solutions when IPv6 usage becomes more widespread.

Goal 4: Promote and support coalitions between the security, infrastructure, and operational technology communities domestically and around the world.

To enhance the resilience of the Internet and communications infrastructure, coordinated actions that cross geopolitical, public-private, industrial sector, and technical boundaries must become easier to implement. This section identifies key actions to increase engagement between critical stakeholder communities.

Action 4.1 ISPs and large enterprises should increase information sharing with government agencies and with one another to provide more timely and actionable information regarding automated, distributed threats.

While many of the actions in this report will increase the cost or reduce the effectiveness of automated, distributed attacks, law enforcement actions have unique impacts on the botnet community. By taking down command and control systems, law enforcement can rapidly “lobotomize” a distributed threat. Prosecution of key players in the botnet economy not only slows the development of distributed threats by current participants, but also discourages prospective developers from joining.

Law enforcement relies on large and small ISPs, incident response teams, cybersecurity and incident response companies, anti-virus vendors, commercial entities, and cyber threat intelligence companies to support ongoing investigations and other efforts to counter automated threats by providing actionable information about threats and trends affecting their networks and customers. By providing even more timely and actionable information, ISPs and other key infrastructure providers can facilitate, support, and accelerate law enforcement actions, including those that affect botnets distributed across the

globe. For example, stakeholders have suggested that expanding incident reporting to include unsuccessful attacks could provide early warnings and support earlier intervention by law enforcement. This type of data would also help the security community better understand the risk landscape.

Law enforcement can proactively identify what kinds of data will help them investigate and prosecute bad actors, and work with infrastructure providers to make it cheaper and easier to share this information with government while protecting Internet user privacy.[82] Improving cybersecurity information sharing continues to be one of the key elements for preventing and mitigating current and emerging cyber-crime issues. To promote trust and broader relationships that have proven useful, law enforcement should continue outreach efforts with the security and network communities to help them identify and understand the right partners in government.

Government agencies, including law enforcement, should continue to improve the timeliness and relevance of cybersecurity information it shares in order to prevent and mitigate cyber incidents. Law enforcement treats companies that have suffered an intrusion or distributed attack as victims of a crime, and conducts their investigations of such reported crimes with discretion to avoid the unwarranted release of information concerning the incident, whenever possible. In addition, private organizations should share cybersecurity information within their industries through Information Sharing and Analysis Organizations and with government agencies where appropriate, while clearly identifying what information should be shared with other entities to prevent additional harm.

RIRs and registrars can facilitate attribution of bad actors by maintaining accurate WHOIS databases. In addition, the federal government should work to engage with its European counterparts to ensure that timely access to WHOIS information is preserved as the European data privacy protections are enforced to preserve a critical tool for domestic and global efforts to investigate botnets. Governments can work with private-sector entities responsible for compliance with data privacy protection regulations, as well as with those entities involved in botnet investigatory work, to ensure that both equities are preserved (compliance and botnet investigations).

Action 4.2 The federal government should promote international adoption of best practices and relevant tools through bilateral and multilateral international engagement.

Significant enhancements to the resilience of the ecosystem cannot be achieved through domestic action alone. The United States should engage regularly with international partners on cybersecurity bilaterally, regionally, and internationally by leveraging expertise within the federal agencies. For issues related to the DNS, NTIA should coordinate with federal agencies and represent U.S. positions at multistakeholder fora, such as the Internet Corporation for Assigned Names and Numbers (ICANN) and Internet Governance Forum.

International standardization could be particularly beneficial. International standards for IoT products and services as well as standards that might otherwise disrupt automated, distributed attacks could expand the market for products that contribute to the resilience of the ecosystem. As the NSTAC report recommended, industry and federal agencies that participate in standards development should

[82] *See*, *e.g.*, Information Sharing and Analysis Organization (ISAO) Standards Organization, *ISAO SP 4000: Protecting Consumer Privacy in Cybersecurity Information Sharing v1.0*, (July 26, 2017), https://www.isao.org/products/isao-sp-4000-protecting-consumer-privacy-in-cybersecurity-information-sharing-v1-0/.

coordinate on a strategy for engaging within appropriate industry-driven international standards bodies to ensure U.S. representation and leadership, and through that participation, champion a flexible and interoperable suite of international standards for IoT security.

Action 4.3 Sector-specific regulatory agencies, where relevant, should work with industry to ensure nondeceptive marketing and foster appropriate sector-specific security considerations.

Due to the complexity and diversity across the IoT landscape, it is difficult to envision a set of one-size-fits-all rules that could ensure security while keeping pace with the rate of change and the dynamic nature of the threat environment. Sector-specific regulatory agencies can, however, promote ecosystem resilience by working with industry to ensure that the security of the products deployed is appropriate for the products' use. For example, the Food and Drug Administration has established guidelines for medical devices that decouple basic security updates from existing product certification regimes.[83] These guidelines are beneficial to consumers, as the medical devices they rely on become more resilient against cybersecurity threats, and to manufacturers, who gain clarity regarding certification requirements. Stakeholders emphasized that the federal government might benefit from an interagency IoT coordination mechanism to promote and share these types of innovative practices and lessons learned, and to avoid regulatory conflicts.

Careful enforcement actions can benefit consumers and honest participants in the market. The FTC has taken action in numerous privacy and security-related cases, with IoT devices figuring in some of these enforcement actions.[84] By halting and deterring deceptive marketing, the FTC can enhance consumer confidence in security claims by IoT and information technology vendors and support positive market incentives. The FTC has also used its unfairness authority under Section 5 of the FTC Act to challenge unreasonable security practices, including in the IoT space. In addition, sector-specific agencies, such as the U.S. Department of Health and Human Services, enforce information security regulations across the relevant industries. These policies can contribute to, and benefit from, the broader ecosystem security discussion.

Action 4.4 The community should identify leverage points and take concrete steps to disrupt attacker tools and incentives, including the active sharing and use of reputation data.

Many threats stem from asymmetries that favor attackers by distributing the exploitation across diffuse actors in the ecosystem. Defenders can use data and information-sharing measures to track attacker tools and can use the incidence of harm to identify tools and actors. In some cases, relatively light coordination efforts should be able to disrupt broader attack classes. Section 3.3 highlights the importance of organizations identifying reflectors that amplify DDoS attacks. The community can track the presence of these threats to help target awareness and threat reduction. Such sharing has helped in addressing threats such as spam, and can be leveraged against other attack vectors.

---

[83] Food and Drug Administration, *Postmarket Management of Cybersecurity in Medical Devices*, (Dec. 28, 2016), *available at* https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

[84] *See, e.g.*, Federal Trade Commission, *In the Matter of TRENDnet, Inc.*, FTC Matter/File Number 122 3090, https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter (last updated Feb. 7, 2014).

"Fast flux hosting" is the automated, rapid modification of IP addresses assigned to hosts in the DNS to hide the location of websites supporting malicious, illegal, or criminal activities. A 2008 Security and Stability Advisory Committee (SSAC) Advisory[85] considered measures that certain registrars and registries implement today: monitoring changes to DNS records that are indicative of fast flux hosting, restricting DNS change frequencies and value ranges, and monitoring registrant account access to prevent automation. It further considered how registrars could apply such measures to expedite suspension processes for illegal websites and domain names. These measures could make a substantial difference in the efforts to curb botnet activity, but they have not been widely implemented. New advances by attackers, including "double flux networks," require further innovation and collaboration at the network level. The broader community, including the federal government, should advocate within the relevant multistakeholder fora (*e.g.*, ICANN and the RIRs) for wider implementation of these measures, or alternative mechanisms to achieve this objective.

Some ecosystem threats are driven by particular illicit markets. The active DDoS-for-hire market is flourishing in gaming communities. Collaboration between gaming companies and payment processors can potentially track and punish those who use these services, drying up the market. Similarly, the market for stolen credentials can be disrupted by making data validation harder.[86] The use of basic anti-automation tools on the web can raise the cost to attackers of verifying the value of stolen credentials, thus reducing the profit from their theft and use. More broadly, research suggests that targeting upstream partners with notification of exposed vulnerabilities can play a key role in driving remediation.[87]

Government investment can be another lever. Agencies have been responsive to metrics and transparency around security issues such as HTTPS adoption.[88] With some guidance and curation, network hygiene reputation could be included as a factor in the government acquisition process. The UK government has begun to experiment with this approach.[89]

Action 4.5 The cybersecurity community should continue to engage with the operational technology community to promote awareness and accelerate incorporation of cybersecurity technologies.

The incorporation of networking functionality into operational technology (OT) (*e.g.*, SCADA systems in industrial settings) has introduced new cybersecurity challenges that can be addressed only through the combined expertise of the cybersecurity and OT communities. The primary requirements associated with instances of OT are often out of scope for cybersecurity subject matter experts, and OT subject matter experts are often unfamiliar with basic cybersecurity practices.

---

[85] ICANN Security and Stability Advisory Committee, *SAC 025: SSAC Advisory on Fast Flux Hosting and DNS*, (Mar. 2008), https://www.icann.org/en/system/files/files/sac-025-en.pdf.
[86] *See* Timothy Peacock & Allan Friedman, *Automation and Disruption in Stolen Payment Card Markets*, (2014), *available at* http://www.econinfosec.org/archive/weis2014/papers/PeacockFriedman-WEIS2014.pdf.
[87] *See*, *e.g.*, Orcun Cetin, Carlos Gañán, Maciej Korczyński & Michel van Eeten, *Make Notifications Great Again: Learning How to Notify in the Age of Large-Scale Vulnerability Scanning*, (2017), *available at* http://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/05/WEIS_2017_paper_17.pdf.
[88] *See*, *e.g.*, Eric Mill, *Tracking the U.S. Government's Progress on Moving to HTTPS*, General Services Administration – 18F, (Jan. 4, 2017), https://18f.gsa.gov/2017/01/04/tracking-the-us-governments-progress-on-moving-https/.
[89] *See* Ian Levy, *Active Cyber Defence—One Year On*, UK National Cyber Security Centre, (Feb. 5, 2018), *available at* https://www.ncsc.gov.uk/information/active-cyber-defence-one-year.

The federal government can facilitate this process by expanding current engagements that bring the cybersecurity and OT communities together to share knowledge and expertise and that promote awareness and accelerate adoption of technologies from the cybersecurity community. Sector-specific agencies work closely with their sectors to understand cybersecurity risk, to link sectors to federal resources, and to promote resilience planning. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors and collaborates with international and private-sector computer incident response teams (CIRTs) to share control systems-related security incidents and mitigation measures. The federal government's cybersecurity community is currently pursuing device-specific engagements with specific OT communities, on topics such as secure updates for infusion pumps. The OT community should participate in the industry actions cited in this report to drive sector-specific solutions to their individualized cyber risks.

Goal 5: Increase awareness and education across the ecosystem.

To enhance the resilience of the Internet and communications ecosystem against distributed threats, all stakeholders must understand and be prepared to execute their roles and responsibilities. This section identifies actions specific to distributed threats that would close gaps between current skills and responsibilities.

These proposed actions do not replace general efforts to increase cybersecurity awareness and education. Stakeholders have indicated that these broad cybersecurity awareness and education initiatives are critical to increasing the resilience of the ecosystem in a sustainable fashion. For example, the importance of beginning cybersecurity education early in the K-12 process was highlighted repeatedly in public comments and contributions in meetings and workshops.

The National Initiative for Cybersecurity Education[90] (NICE), led by NIST in the U.S. Department of Commerce, is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. Its mission is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development, with a focus on cybersecurity workers. Programs range from K-12 cybersecurity education and collegiate academic pathways, such as the National Centers of Academic Excellence in Cybersecurity,[91] to the development and management of performance-based evaluation and training programs. The Department of Homeland Security complements NICE's contributions, playing a vital role in awareness efforts through the STOP. THINK. CONNECT.[92] program.

The following actions build upon these more general cybersecurity awareness and education efforts, identifying awareness and educational opportunities specifically related to mitigation or prevention of distributed threats.

[90] National Initiative for Cybersecurity Education, National Institute of Standards and Technology, https://www.nist.gov/itl/applied-cybersecurity/nice (last visited Apr. 4, 2018).
[91] Centers of Academic Excellence in Cybersecurity, National Security Agency, https://www.nsa.gov/resources/educators/centers-academic-excellence/ (last visited Apr. 10, 2018).
[92] Stop. Think. Connect., https://www.stopthinkconnect.org/ (last visited Apr. 4, 2018).

Action 5.1 The private sector should establish and administer voluntary informational tools for home IoT devices, supported by a scalable and cost-effective assessment process, that consumers can trust and intuitively understand.

The private sector, in consultation with civil society and government experts, should devise an efficient and effective assessment and labeling approach for IoT devices so security-conscious consumers can make informed choices and create market incentives for secure-by-design product development. Many commercially available IoT products were not designed with security in mind. These devices create a systemic risk for all members of the ecosystem, and place consumers' privacy and security at risk. In an ideal world, consumers would prefer IoT products that also protect their security and privacy, but security-conscious consumers cannot easily identify which IoT products were designed to be secure. Without this information, their selection criteria are limited to the price and feature set.

The private sector is best suited to the creation and maintenance of lightweight and agile mechanisms, but can often benefit from government's convening power. The federal government should convene industry, civil society, and government stakeholders in a multistakeholder process to explore requirements for a viable labeling approach. This effort can build on initial successes of programs like NTIA's multistakeholder process on IoT Security Upgradability and Patching, which produced a document detailing the key elements that manufacturers should consider communicating to consumers both before and after purchase.[93] Stakeholders should consider whether a mechanism that relies on vendor assertion is viable and meets home consumer needs. Viability of such a mechanism could rely in part on existing prohibitions against commercial deception. For instance, the Federal Trade Commission could protect the integrity of the assessment mechanism by taking action against deceptive marketing (*e.g.*, false compliance claims), understanding that security assurances in this space cannot offer similar guarantees compared to safety assertions that remain static over time. DHS could also support the assessment program through its existing awareness activities, such as STOP. THINK. CONNECT. (See Action 5.3).[94]

While IoT security and privacy is not perfectly analogous, mechanisms such as the NHTSA 5-Star Safety Rating and Energy Star programs have successfully raised customer awareness and created markets for safe vehicles and energy-efficient appliances, supporting the hypothesis that a well-conceivable labeling approach would help reduce automated and distributed attacks. However, the large number of different IoT devices and the relatively brief sales period for many of these devices (in comparison with cars and water heaters) indicates that a lighter weight and more agile mechanism will be required. Given the global nature of business today, the assessment scheme should be based on internationally recognized standards wherever possible. Further, any use of a security assessment and labeling approach would need to reflect the differences between safety assertions, which remain static over time, and security assertions, which cannot offer similar guarantees. DHS could complement such broadly applicable mechanisms by exploring opportunities regarding a certification regime that may be effective in supporting the needs of critical infrastructure.

There is also a role for subjective assessment of IoT devices and their usability. Consumer-oriented testing organizations often supplement feature-based analysis and repair histories with more subjective assessments of comfort or usability. Usability of management interfaces for security is a particularly

[93] NTIA Multistakeholder Process on Internet of Things Security Upgradability and Patching, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security (last updated Nov. 7, 2017).
[94] Stop. Think. Connect., https://www.stopthinkconnect.org/ (last visited Apr. 4, 2018).

difficult problem. By including thoughtful assessments of usability, consumer-oriented testing organizations can help consumers identify the products that are appropriate for their skill levels.

Action 5.2 The private sector should establish voluntary labeling schemes for industrial IoT applications, supported by a scalable and cost-effective assessment process, to offer sufficient assurance for critical infrastructure applications of IoT.

Critical infrastructure and industrial applications of IoT present significantly higher risks to the nation than home applications in the context of automated, distributed attacks. These devices are also deployed in very different environments, supported by professional administrators. The voluntary lightweight assessment mechanism envisioned in Action 5.1 would not offer a sufficient level of assurance for these customers, and additional features are likely to be required. Assessment features such as device authentication, hardware roots of trust, or managed update functions would require direct interaction with products, if not review of source code.

Examples of success for such a process exist in both the government and the private sectors. For example, NIST's Cryptographic Module Validation Program has leveraged independent testing laboratories to assess the security of cryptographic modules against the Federal Information Processing Standards (FIPS) 140 standard for more than two decades. In the private sector, safety and certification company UL has a variety of certification and compliance schemes for both commercial and consumer markets, with more than 20 billion UL marks appearing on products in 2016. However, fragmented or overly complex labeling can backfire. The FTC, with its considerable expertise in labeling, supports clear disclosures but cautions that "poor disclosures, including overly extensive disclosures, can actually impede consumers' ability to make informed choices."[95]

The private sector should establish an efficient but robust evaluation process to ensure that IoT devices for these sectors offer enhanced resilience at an appropriate level of assurance. Establishing an evaluated products list will permit security-conscious enterprises to make informed choices and create market incentives for robust secure development lifecycle processes.

Action 5.3 Government should encourage the academic and training sectors to fully integrate secure coding practices into computer science and related programs.

As noted in Action 1.3, many common security vulnerabilities (*e.g.*, buffer overflows) can be avoided or remedied during product development by applying appropriate security development tools, such as fuzzers, static analyzers, and safe programming languages. While academic institutions, coding boot camps, and job retraining programs are creating a larger coding workforce, their graduates are rarely skilled in these languages or adept at using these development tools. Instead, students gain significant experience with software development tools that do not consider security, and software development methodologies that do not prioritize security, creating a bolt-it-on-later mindset among the software development workforce.

Companies that wish to improve coding practices may be deterred by an unprepared and sometimes resistant workforce—skilled coders can easily change jobs if they are not interested in learning the new

[95] Federal Trade Commission, *Public Comment on "Communicating IoT Device Security Update Capability to Improve Transparency for Consumers,"* at page 6, (2017), *available at* https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-comment-national-telecommunications-information-administration-communicating-iot-device-security/170619ntiaiotcomment.pdf.

practices, and can be challenging to replace. By teaching secure-by-design software methodologies and encouraging use of security-aware software development toolchains throughout the computer science and cybersecurity-related curriculum, we can prepare our workforce to build higher-quality software and increase acceptance of security-focused software development toolchains.

The federal government can facilitate these changes through existing relationships with academia and the training industry. In particular, NICE should engage with academia and the private sector to incorporate secure-by-design principles and supporting tools at every step in the course of study. The NICE Cybersecurity Workforce Framework (NICE Framework) category of "Securely Provision" includes the knowledge, skills, and abilities that are needed for secure software and product development. NICE should partner with educational and training providers to encourage them to use the NICE Framework as a reference tool for the development of course content. As another example, the FTC hosts an annual PrivacyCon conference, which provides a showcase for privacy and security work by academics and security researchers.[96]

Action 5.4 The academic sector, in collaboration with the National Initiative for Cybersecurity Education, should establish cybersecurity as a fundamental requirement across all engineering disciplines.

As IT is integrated into the full range of products and services, cybersecurity threats arise in new classes of products. Product designers are often unaware of the risks that can be introduced when integrating IT into traditional product lines. The need is growing for these workers to understand cybersecurity risk management, as we embed sensors in numerous environments, including soil, highways, and buildings. For example, closed circuit television (CCTV) cameras have been available commercially since 1949, but only recently evolved into Internet-connected devices. In 2016, the Mirai botnet compromised more than 100,000 CCTV cameras to support DDoS attacks. In other cases, Internet-connected cameras used as baby monitors have been hacked by exploiting default administrative passwords, violating the owners' privacy.[97]

To ensure that product designers are aware of the risks introduced into operational technology, academic institutions teaching engineering and related disciplines should integrate basic cybersecurity into the required curriculum. As above, NICE should engage with academia and the private sector to incorporate principles into the course of study for engineering and related disciplines.

Action 5.5 The federal government should establish a public awareness campaign to support recognition and adoption of the home IoT device security baseline and branding.

To achieve impact, the home IoT device security baseline must be recognized and preferred by security-conscious consumers, enhancing the resilience of home networks where the devices are installed and establishing market incentives for security-conscious vendors. The federal government has a long history of public awareness campaigns, pursued with stakeholder support, to address a wide variety of topics: how to prevent forest fires, the value of seatbelts, and the importance of HIV testing. The Stop. Think. Connect. campaign is a DHS-sponsored national public awareness campaign aimed at increasing the

[96] *See* Federal Trade Commission, *PrivacyCon 2018*, https://www.ftc.gov/news-events/events-calendar/2018/02/privacycon-2018 (last visited Apr. 4, 2018).
[97] *See* Darlene Storm, *Hacker Hijacks Wireless Foscam Baby Monitor, Talks and Freaks Out Nanny*, Computerworld (Feb. 2, 2015, 12:09 PM PT), https://www.computerworld.com/article/2878741/hacker-hijacks-wireless-foscam-baby-monitor-talks-and-freaks-out-nanny.html.

understanding of cyber threats and empowering the American public to be safer and more secure online. The federal government should consider leveraging Stop. Think. Connect. or establishing a complementary public awareness campaign to alert home users and small organizations to the importance of the home IoT device baseline and educate them on how to identify more secure products. More generally, enhanced user awareness of cybersecurity risk is critical to a resilient ecosystem, and government should increase its strategic engagement and convening power with targeted user communities and civil society to improve security adoption and awareness, welcoming any nongovernmental stakeholders that wish to play a larger role.

* * *

Initial Next Steps for Stakeholder Action

The section above details 24 actions designed to achieve five goals. The five goals are mutually supportive; all five goals must be achieved to sustainably increase the resilience of the Internet and communications ecosystem. Many of the actions are also mutually supportive by design, even across goals, so excluding or omitting an action could potentially delay achieving multiple goals. However, we do not expect all actions to occur simultaneously, due to considerations such as resource constraints in the relevant stakeholder communities. In addition, some actions are already in progress, while others are dependent on outside factors. The federal government will not lead the implementation of actions specific to industry. However, understanding that in some cases it may take time for the private sector to organize, the U.S government will immediately begin coordinating the initial steps outlined below.

Develop a prioritized road map for coordinated actions to increase the resilience of the Internet and communications ecosystem against distributed threats.

To ensure that the most important actions are adequately resourced and efficiently executed by stakeholders, the stakeholder communities have strongly encouraged the federal government to clearly delineate priorities for action.[98] In particular, some actions 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.

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. Other actions are ripe for prioritization because the preparatory work is underway, such as the 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 developments are narrowing the window for the United States to influence the direction (Action 1.2).

The Departments of Commerce and Homeland Security, in coordination with industry, civil society, and in consultation with international partners, should be tasked with developing an initial road map with prioritized actions within 120 days after approval of this report. This road map should align with

[98] This request was highlighted both in stakeholder responses to the January 5, 2018, Request for Comment as well as the February 28-March 1, 2018, workshop.

Administration priorities as set forth following the completion of tasks assigned under Executive Order 13800. Government and the private sector will work together to ensure that the road map is updated and maintained as stakeholders accomplish the identified actions.

The federal government will lead by example.

Stakeholders indicated that federal leadership by example is critical to implementation of the report by other stakeholders. Stakeholders indicated that federal adoption of "good neighbor" practices that primarily benefit the ecosystem and procurement activities would provide a 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. NIST, OMB, and DHS should explore steps to ensure that these best practices are properly reflected in federal agency policies, standards, guidelines, and oversight.

Similarly, federal procurement activities mandating acquisition of products and services that are more secure or resilient than commonly available today were viewed as an important step toward establishing market incentives. Stakeholders suggested an immediate focus on the actions 1.1, 1.2, and 2.3 to support federal procurement guidance. This design work can then lead to an evaluation of existing procurement guidance and standards, as well as specific recommendations for updating that guidance to reflect secure requirements.

Foster private-sector leadership and support cross-sector coordination to track implementation of the road map.

Many of the road map actions should be led by an industry sector, academia, or civil society. Identification or establishment of private-sector governance structures for these activities will be a critical factor in sustainability and international acceptance of work products (*e.g.*, technical specifications or assessment schemes). Where existing bodies are already pursuing related actions, or already represent key communities, they should be encouraged to lead. Actions may require inclusivity beyond current structures—for example, adding civil society or international participants or perspectives.

As communities form to implement these actions, establishing a venue for regular coordination between these communities will be increasingly important. The value of an IoT security baseline is limited if an assessment scheme cannot be established in a timely manner. Alignment and coordination of investments is needed to maximize impact on the resilience of the infrastructure. Until a mutually agreed party or parties from the private sector are identified, the federal government will provide a coordination and communication mechanism for continued implementation, and will convene periodic meetings of the relevant parties.

Provide a 365-day status report to the President on road map implementation.

To track progress, the Departments of Commerce and Homeland Security 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) whether any adjustments are required to the road map.

Promote global participation through enhanced stakeholder and U.S. government engagement on international policy and standards development.

The global nature of distributed threats was frequently highlighted during the process executed by Commerce and Homeland Security. Stakeholders highlighted the importance of international standards, policies, and best practices in promoting international participation and collaboration. By continuing to advocate for industry-led approaches and by actively participating in development of voluntary, consensus-based international standards, the federal government can contribute to pragmatic and effective outcome-based standards that meet the needs of all stakeholders. The federal government is also uniquely positioned to lead the international engagement required to establish broadly accepted policies and best practices and will enhance coordination with stakeholders on these efforts.

Appendix: Acronym List

AI	Artificial intelligence
BCP	Best Current Practice
BGP	Border Gateway Protocol
CCTV	Closed circuit television
CDN	Content delivery network
CIRT	Computer incident response team
CISA	Cybersecurity Information Sharing Act of 2015
CSF	NIST Cybersecurity Framework
CSIRT	Computer Security Incident Response Team
CSRIC	Communications Security, Reliability and Interoperability Council
DDoS	Distributed denial of service
DHS	Department of Homeland Security
DNS	Domain Name System
FIPS	Federal Information Processing Standards
FIRST	Forum of Incident Response and Security Teams
FTC	Federal Trade Commission
GSA	General Services Administration
HTTPS	Hypertext Transfer Protocol Secure
ICANN	Internet Corporation for Assigned Names and Numbers
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISAC	Information sharing and analysis center
ISP	Internet service provider
IT	Information technology
LAN	Local area network
MANRS	Mutually Agreed Norms for Routing Security
MUD	Manufacturer's Usage Description
NAT	Network address translation
NCC	National Coordinating Center for Communications
NCCIC	National Cybersecurity and Communications Integration Center
NHTSA	National Highway Traffic Safety Administration
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency/Internal Report
NITRD	Networking and Information Technology Research and Development
NOG	Network operator group

NSTAC	President's National Security Telecommunications Advisory Committee
NTIA	National Telecommunications and Information Administration
OT	Operational technology
PPD	Presidential Policy Directive
RFC	Request for Comment
RIR	Regional Internet Registry
SAM	Software asset management
SCADA	Supervisory control and data acquisition
SSAC	Security and Stability Advisory Committee