A Submission from Cloudflare, Inc., in response to

"Request for Comment on Promoting Stakeholder Action Against Botnets and Other Automated Threats"

A Notice by the National Telecommunications and Information Administration on 01/05/2018

Cloudflare welcomes the leadership of the Department of Commerce and the Department of Homeland Security in addressing botnets and other cybersecurity challenges. We believe that the report of January 5, 2018, and its invitation to continue the discussion about specific actions that can reduce the threat posed by botnets will be particularly helpful in spurring both government agencies and private companies to invest more time and effort in an area that too often receives too little attention. We are very glad to see that the report builds on the NIST Cybersecurity Framework and the useful reports from the National Security Telecommunications Advisory Council (NSTAC) and the National Commission on Enhancing Cybersecurity (chaired by Thomas Donilon and co-chaired by Sam Palmisano).

Cloudflare is an Internet performance and security company working to build a better Internet, and has been a leader in identifying and limiting the damage done by botnets. We protect more than seven million web properties around the world from Distributed Denial of Service (DDoS) attacks. With over 120 data centers in more than 58 countries, we serve approximately 10% of global Internet requests, which is more web traffic than Twitter, Amazon, Apple, Instagram, Bing, & Wikipedia combined. Every week, the average Internet user travels through our network more than 500 times. In a typical day, the Cloudflare network of data centers blocks more than 400 million DDoS attacks. This gives us a unique perspective on where botnets are located and how they are being used to launch DDoS attacks.

ENSURING A COMPREHENSIVE APPROACH

The report provides a comprehensive and global perspective, addressing the role of every component of the Internet infrastructure and recognizing that "no single tool can secure the infrastructure" against botnets and automated attacks. It discusses a wide range of possible actions that can help reduce the number of botnet attacks and mitigate the damage they cause. But it can do more than that. It can push back more forcefully against misperceptions limiting proposed solutions to the problems posed by botnets. It would be useful for the final report to more explicitly state just how complex and difficult the botnet challenge will be to address effectively. We believe it would be very helpful to place more emphasis on how:

1) *The threat posed by botnets does not stem solely from computers and Internet of Things devices (e.g. the CCTV cameras and VDRs used in the Mirai botnet attacks).* We also need to pay attention to the traffic coming from misconfigured or compromised network servers and from Cloud computing services.
2) *Most DDoS attacks target individuals and small businesses--even though most of the news reports about botnet attacks focus on attacks on large organizations like banks and financial services companies, IT and media websites, governments, or political campaigns.* Every day, Cloudflare hears from small businesses and individuals whose websites are knocked offline by cyber-extortionists who will stop their attacks if paid "protection money" in cryptocurrency. Fortunately, affordable tools to block such attacks are readily available. (That is one reason cyber-extortionists are shifting their focus to using ransomware and to stealing data for ransom.)
3) *The companies fighting against DDoS attacks are making progress.* Recent data from late 2017 from both Cloudflare[1] and Verisign[2] indicate that the size and frequency of DDoS attacks are decreasing. Unfortunately, they are becoming more complicated and sophisticated. As Layer 3 and Layer 4 attacks are mitigated more effectively, Layer 6 and Layer 7 attacks are becoming more serious.
4) *Solving the problem of botnet attacks, particularly those coming from IoT devices, is going to require much more work outside the United States than in the US.* The large majority of Internet users connect to the Net via a non-American Internet Service Provider. Most of the devices on the Internet are manufactured outside the US--and many of them are designed there, too. Global solutions to the threats posed by botnets require global collaboration.
5) *It's not just about technology, better business practices, information sharing, and law enforcement.* It's also about marketing and economics. We share the report's conclusion that we already have many of the tools and technologies we need to make DDoS attacks more difficult and less lucrative for cyber-criminals; we need more education and marketing to spur deployment of those tools.

[1] 2018 and the Internet: our Predictions, Cloudflare Blog, https://blog.cloudflare.com/our-predictions-for-2018

[2] Distributed Denial of Service Trends Report, Verisign, https://www.verisign.com/en_US/security-services/ddos-protection/ddos-report/index.xhtml

6) *It is critical that more effort goes into making DDoS protection simple and easy to use.* Cloudflare believes that in a few years, DDoS protection will be seamlessly integrated with the Cloud. Using software at the edge, rather than having to manage hardware, has enabled millions of website owners to quickly protect themselves.

SETTING PRIORITIES

Some of the actions in the report have the potential to be both highly effective and require relatively little effort. But, in order to ensure that Federal government (and private sector) initiatives address the right challenges and are implemented effectively, there must be a shared understanding of which proposals are likely to provide the greatest benefits and how long it will take to realize those benefits.

The remainder of this submission provides our qualitative assessment of each of the 23 proposed actions listed in the report. For each one, we assess how much the proposed action will help deal with the threat of botnets, how difficult it will be to do, and how long before benefits are seen. We also describe how governments and industry could work together to maximize the benefits and achieve them as quickly as possible.

While Cloudflare will not be directly impacted by or involved in all of the proposed actions, we felt it would be useful to comment on each one of them because we are part of the cybersecurity industry and the broad Internet community. It is also important to stress that several of the proposed actions can be justified for many reasons, not just because they will help reduce the threat of botnets. This is particularly true of the actions listed under Goal 5, “Increase awareness and education across the ecosystem.” These actions will improve our technical workforce and result in better-informed Internet users, which could help the entire tech sector and accelerate the deployment of digital technologies in all sectors of the economy. The tables flag those proposed actions with broader impact (beyond botnet mitigation). It is also key to stress, as the report does, that many of the proposed actions are linked. For instance, initiatives to develop guidelines and proposals will have a much greater impact if actions to educate IT professionals and technology buyers are effective.

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

Cloudflare supports all the actions proposed under Goal 1 because they will spur innovation and increase the market forces that drive development and deployment of better cybersecurity technologies. Government has a particularly important role funding long-term fundamental research, training graduate students, and making markets more transparent and competitive.

Action	**Benefit**	**Difficulty**	**Time**	**Impact**
Action 1.1 Establish broadly accepted baseline security profiles for IoT devices in home and industrial applications, and promote international adoption through bilateral arrangements and the use of international standards. The federal government should accelerate this process by adopting baseline security profiles for IoT devices in U.S. government environments.	Med.	High	Long	Med.
Action 1.2 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.	High	Low	Med.	Broad
Action 1.3 Industry should expedite the development and deployment of innovative technologies for prevention and mitigation of distributed threats. Accordingly, where applicable, government should prioritize the application of research and development (R&D) funds and technology transition efforts to support advancement in DDoS prevention and mitigation, as well as foundational technologies to prevent botnet creation.	High	Low	Long	Med.
Action 1.4 Government and industry should collaborate to ensure existing best practices, frameworks, and guidelines relevant to IoT, as well as procedures to ensure transparency, are more widely adopted across the digital ecosystem.	High	Low	Med	Med.

Action 1.1 Establish broadly accepted baseline security profiles for IoT devices in home and industrial applications, and promote international adoption through bilateral arrangements and the use of international standards. The federal government should accelerate this process by adopting baseline security profiles for IoT devices in U.S.

government environments.

The proposed action is important because it leverages the Federal government's role in standards development and its "power of the purse" to promote the development and deployment of more secure Internet of Things devices. While IoT devices generate a small fraction of total DDoS traffic today, that fraction is growing, so there is a need to move quickly on this proposal--particularly because the proposed profile must be embraced by IoT device manufacturers around the world, and that will take time.

It is also critical that the profile for IoT devices not be a mandatory compliance checklist but rather be designed like the original NIST Cybersecurity Framework, which identified challenges to be addressed and provided resources about the various ways to tackle those challenges. Furthermore, it is essential that the profile recognize the full range of IoT devices, from million-dollar machine tools to twenty-cent sensors. Accordingly, it will be important to realize that often the best way to protect a simple IoT device is not by adding extra hardware or software on the device itself but rather by ensuring that it can only connect to the Internet through a secure gateway or virtual private network. A secure Internet connection ensures both that the device is protected from attack and that the device cannot be compromised or used to generate DDoS traffic.

Action 1.2 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.

Like several other proposed actions in this report, this one could have a positive impact far beyond the narrow area of botnet mitigation. The good news is that it would not be very costly. The bad news is that it involves changing how developers do their jobs. And that requires finding ways to put a spotlight on companies and developers who are not using effective tools and techniques to identify vulnerabilities in software. That is why we welcome the emphasis on "transparency tools." We also are glad to see the emphasis on evaluating software components, libraries, and modules, since many IoT devices use old, recycled code. Cloudflare has built much of its infrastructure on open-source software and has always worked hard to avoid old, buggy versions and to work with the open-source community to identify and fix vulnerabilities in the versions of the code we use.

Action 1.3 Industry should expedite the development and deployment of innovative technologies for prevention and mitigation of distributed threats. Accordingly, where applicable, government should prioritize the application of research and development (R&D) funds and technology transition efforts to support advancement in DDoS prevention and mitigation, as well as foundational technologies to prevent botnet creation.

Decades of government and corporate support for a broad base of computer science and engineering R&D is one reason the United States has been a world leader in information technology. Federal government research programs not only generate technological breakthroughs. By funding graduate students at our universities, they fund the development of the talent that companies like Cloudflare rely upon. But the benefits often take many years to become obvious and can be very hard to quantify,

Action 1.4 Government and industry should collaborate to ensure existing best practices, frameworks, and guidelines relevant to IoT, as well as procedures to ensure transparency, are more widely adopted across the digital ecosystem.

This proposed action is essential if the other three actions under Goal 1 are to have a major impact. The best advice is not useful if no one hears it, so marketing is key. We are glad to see a commitment to working with both vendor and user communities to “spread the word.”

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

Cloudflare feels that the most cost-effective and fastest way to address the rapidly-evolving threat posed by botnets is by deploying better means to block DDoS traffic from reaching its targets. We are particularly supportive of Action 2.2, which, if it leads to voluntary, widely-accepted, flexible guidelines, could encourage hundreds of thousands of companies and organizations--both in the United States and elsewhere--to prevent and mitigate against DDoS attacks.

Action	Benefit	Difficulty	Time	Impact
Action 2.1 Internet service providers and their peering partners should expand current information sharing to achieve more timely and effective sharing of actionable threat information both domestically and globally.	Med.	Low	Short	Med.
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.	High	Low	Med.	Narrow
Action 2.3 The federal government should lead by example and demonstrate practicality of technologies, creating market incentives for early adopters.	Med.	Med.	Short	Med.
Action 2.4 Industry and government should collaborate with the full range of stakeholders to continue to enhance and standardize information-sharing protocols.	Low	Med.	Med.	Med.
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.	Low	High	Med.	Broad

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

This proposed action seems incomplete because it focuses only on ISPs and network providers. Many ISPs, especially smaller ones, rely on companies that provide network security services, such as Cloudflare and Google, to identify and block botnet traffic. Network security companies and ISPs already have open lines of communication and are able to respond quickly when a new major DDoS threat develops. The best example of this was when the first Mirai botnet attacks[3] were launched. Assessments and counter-measures[4] began immediately[5]--and involved the key players. The final report should make clear that the extensive amount of

[3] Inside the infamous Mirai IoT Botnet: A Retrospective Analysis, Cloudflare Blog https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/

[4] The New DDoS Landscape, Cloudflare Blog, https://blog.cloudflare.com/the-new-ddos-landscape/

[5] How Google fought back against a crippling IoT-powered botnet and won, Ars Technica https://arstechnica.com/information-technology/2017/02/how-google-fought-back-against-a-crippling-iot-powered-botnet-and-won/

information sharing that is already occurring and how it involves much more than just ISPs.

This Action might be expanded to include efforts to get Cloud computing providers to redouble their efforts to prevent theft and misuse of their services for botnet attacks. Given the small number of companies in this market segment, it should be relatively easy to make progress in limiting DDoS attacks misusing their services.

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.

For Cloudflare, this is the most important proposed action in the report and the one likely to provide the biggest benefits--if it is done right. Developing a Framework profile will encourage enterprises to think about how to improve their DDoS threat mitigation. We would encourage NIST to consider ways to expand any profile that is developed to smaller businesses as well.

The global reputation of NIST means that it will be able to convene the right experts and stakeholders, just as it did for the original Cybersecurity Framework. Equally importantly, the team at NIST will be able to use their contacts around the world to build awareness of the DDoS prevention profile. However, it is essential that the profile not be designed as a compliance checklist mandating specific products. We know that fighting botnets requires a defense in depth strategy using a variety of weapons and shields from different suppliers to be most effective. Different levels of protection are needed for different types of devices. Different industry sectors have different requirements.

A comprehensive profile should include steps that enterprises can take to prevent their network servers from being exploited for reflection and amplification attacks, which in some cases can increase the amount of traffic generated by botnets 20, 30, or even 50 times. As Cloudflare described in its initial response to the June 2017 Request for Comments[6] on dealing with botnets, this has been a particular problem

[6] Request for Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats, NTIA, https://www.ntia.doc.gov/federal-register-notice/2017/rfc-promoting-stakeholder-action-against-botnets-and-other-automated-threats

at Federal agencies, where misconfigured DNS servers[7] have been routinely exploited in many of the largest DDoS attacks.

It is also essential that the profile not be seen as something that will be mandated for certain classes of users. If it is voluntary and provides a variety of ways for readers to achieve the specific tasks identified, it will be much easier and faster to develop a consensus around the text. NIST knows how to do this and do it in a open, transparent, and international manner. It will be challenging to engage non-US companies and even harder to engage non-US technology customers, but is is essential that this be done from the start to avoid this initiative being seen as an "American solution" to a serious global problem.

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

The US government is a major user of information technology, and can play a significant role in validating and encouraging the use of new technology. Unfortunately, government procurement requirements like FedRAMP can create an artificial barrier prohibiting the government from using new, more cost-effective technologies to defend against botnets if those technologies were not anticipated when the regulations were last revised. To ensure regulations do not disincent early adopters, there should be an easy way for the government to adopt and test such technologies without requiring the time and expense of FedRAMP certifications.

In addition, the Federal government can play an important role by "walking the talk" and by using the Federal IT procurement process to encourage vendors who demonstrate that they are implementing effective steps to protect against DDoS attacks (and to ensure that the systems they deploy and run cannot be used for DDoS attacks). That said, overly prescriptive or overly broad[8] procurement regulations, particularly ones that inadvertently hinder development and use of new, leading-edge solutions, could do more harm than good. Development of cybersecurity technologies is moving much faster than the government can enact regulations and guidelines.

[7] How the Consumer Product Safety Commission is (Inadvertently) Behind the Internet's Largest DDoS Attacks, Cloudflare Blog, https://blog.cloudflare.com/how-the-consumer-product-safety-commission-is-inadvertently-behind-the-internets-largest-ddos-attacks/

[8] Analyzing the Internet of Things Cybersecurity Improvement Act, AEI, http://www.aei.org/publication/analyzing-the-internet-of-things-iot-cybersecurity-improvement-act/

The federal government should also lead the way by ensuring that all of its computers and network servers are properly configured, so that they cannot be used to launch or amplify DDoS attacks.

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

As described above, under Action 2.1, there is already a lot of information sharing happening between network security companies and the other network providers who are best-positioned to detect and analyze where botnets are and where DDoS traffic is targeted, particularly when a new type of attack occurs. The challenge is not to facilitate cooperation among this rather small, trusted community. The challenge is to reach the much broader and more diverse group of organizations that might be on the receiving end of a DDoS attack. They do not need the kind of detailed technical information that network security companies and network providers share when they are trying to identify a new threat. Instead, they need actionable advice about what to do about the threat. Past information sharing initiatives tended to confuse the two needs. To quote one former Federal government official, who now works with the cybersecurity industry, “For too long, we have been asking the wrong people to share the wrong information with the wrong people.” Cloudflare believes this proposed action could be very helpful if it recognized the need for different types of information for different communities. We also believe the largest and most difficult information sharing challenge is to get companies and organizations outside the tech sector, who are so often the easiest targets for DDoS attacks, to take action.

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.

This is a useful but ambitious proposal. It will be challenging to get agreement on what “best practices” are in an area when technology is advancing rapidly and it will be even more challenging to get the full range of Internet infrastructure players to embrace a common approach, if it is too prescriptive. As explained above, there has been a very effective synergy between network security companies like Cloudflare and network providers in which network providers (as well as hosting companies) chose security solutions that work for them (and security companies compete with each to provide better, less expensive, and easier to use solutions.)

Goal 3: Promote innovation at the edge of the network to prevent, detect, and mitigate bad behavior

Cloudflare believes that existing technologies and techniques, if properly deployed, could eliminate at least 80% of DDoS traffic. Therefore, we welcome actions that will accelerate deployment of state-of-the-art network management tools and secure gateways. These approaches, as well as new edge-based approaches, can be much easier to use and more cost-effective.

Action	**Benefit**	**Difficulty**	**Time**	**Impact**
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.	High	Med.	Short	Med.
Action 3.2 User interfaces on home IT and IoT products should be designed to maximize security while reducing or eliminating security knowledge requirements for administration.	High	Low	Med.	Med.
Action 3.3 Enterprises should migrate to network architectures that facilitate detection, disruption, and mitigation of automated, distributed threats.	High	Med.	Med.	Broad
Action 3.4 The federal government should investigate how wider IPv6 deployment can alter the economics of both attack and defense.	Med.	Med.	Short	Med.

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.

Cloudflare is very glad to see this proposed action in the report. Too often, discussions of cybersecurity and the Internet of Things focuses solely on the “things” and forgets that often the best way to secure devices is to secure the way they connect to the Internet (through a secure network hub, gateway, or an edge-based security solution[9]). This kind of holistic approach is essential if the hundreds of billions of IoT devices that will soon be connected to the Internet are to be protected against DDoS attacks (and not be vulnerable to being incorporated into botnets). We hope that these kind of solutions will play a key role in the DDoS

[9] Introducing Cloudflare Orbit: A Private Network for IoT Devices, Cloudflare Blog, https://blog.cloudflare.com/orbit/

prevention profile proposed under Action 2.2.

Action 3.2 User interfaces on home IT and IoT products should be designed to maximize security while reducing or eliminating security knowledge requirements for administration.

This is a critical element of any comprehensive strategy to address the botnet threat. Too often we only focus on security, privacy, and reliability and forget usability is key to realizing those goals. Fortunately, we are making progress. Systems auto-configure and have automatic software updates. The shift from hardware solutions to Cloud-based services is also making life less challenging for CIOs and systems administrators. The chronic shortage of qualified IT professionals, which is growing worse, means this proposed action is critical--and since it will take time for products to diffuse into the market, it is important to move as quickly as possible.

Action 3.3 Enterprises should migrate to network architectures that facilitate detection, disruption, and mitigation of automated, distributed threats.

This important proposed action builds on Action 2.2 which calls for a Cybersecurity Framework profile for DDoS protection. As noted in the report, there are “a variety of effective anti-DDoS products and services”; the challenge is to get enterprises to deploy them. Security companies are spending millions of dollars marketing their products, but having independent industry groups, associations of government IT professionals (at the national, state, and local level), and user groups highlight approaches that work would help buyers sort through the options.

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

Cloudflare is glad to see IPv6 singled out as part of the strategy for mitigating DDoS attacks. We have been promoting adoption of IPv6 since the start of our company more than seven years ago, in part because it provides new and more varied means for improving the cybersecurity and performance of networks. And, of course, it is essential to ensure the continued rapid growth of a secure, reliable Internet of Things.

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

There is already tight collaboration and coordination among those companies and Federal agencies directly involved in identifying and responding to DDoS attacks. More could be done to reach out to ISPs and large enterprises overseas. But the biggest challenge is helping potential victims of DDoS attacks--particularly small and medium-sized companies and organizations that are not in the technical sector--learn how to effectively respond to them.

Action	**Benefit**	**Difficulty**	**Time**	**Impact**
Action 4.1 ISPs and large enterprises should increase information sharing with law enforcement to provide more timely and actionable information regarding automated, distributed threats.	Low	Med.	Short	Narrow
Action 4.2 The federal government should promote international adoption of best practices and relevant tools through bilateral and multilateral international engagement efforts	Med.	High	Long	Med.
Action 4.3 Regulatory agencies should work with industry to ensure non-deceptive marketing and foster appropriate sector-specific security requirements.	Med.	High	Med.	Broad
Action 4.4 The community should take concrete steps to limit fast flux hosting.	Med.	Low	Short	Narrow
Action 4.5 The cybersecurity community should continue to engage with the operational technology community to promote awareness and accelerate cybersecurity technology transfer.	Med.	Med.	Long	Med.

Action 4.1 ISPs and large enterprises should increase information sharing with law enforcement to provide more timely and actionable information regarding automated, distributed threats.

Companies involved in identifying and protecting against DDoS attacks cooperate with law enforcement agencies in efforts to shut down the people controlling the botnets responsible for the attacks. But when the threat comes for millions of machines in almost every country, law enforcement is only a small part of the solution. Botnet herders, like spammers, do not require deep technical skills. If one cyber-criminal is arrested, another will replace him or her.

Network providers and Internet security companies can provide timely information on attacks and attackers, but they must do it in a way that protects their users' privacy. We are glad to see the acknowledgement of concerns about privacy and confidentiality.

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

In the long run, this proposed action could be one of the most important and one of the most difficult. It also builds on several other proposed actions (particularly Action 1.1 and Action 2.2). Securing the Internet requires efforts by network providers, cybersecurity companies, device manufacturers, DNS providers, and others in every country. Thus, we are glad to see the commitment to working with existing international standards bodies and groups like ICANN to promote best practices. But it is essential that such bodies not write narrow standards that lock in yesterday's technologies and techniques.

Action 4.3 Regulatory agencies should work with industry to ensure non-deceptive marketing and foster appropriate sector-specific security requirements.

This section of the report included an important admonition: "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." That said, regulatory agencies that promote a range of solutions to the threat posed by DDoS attacks could help motivate companies to make the necessary investments in securing their IT infrastructure. As noted in the report, the Federal Trade Commission (FTC) has taken action against companies that have failed to practice reasonable security practices.

Action 4.4 The community should take concrete steps to limit fast flux hosting.

Fast flux hosting has been used to make it harder to block DDoS attacks for more than ten years, since the early days of botnets. Clearly, the efforts of ICANN and Regional Internet Registries to motivate key players in the domain name ecosystem to do more to address the problem have been insufficient. Merely highlighting the challenge in the final report may help, but being more specific about exactly who needs to take action would be even more useful.

Action 4.5 The cybersecurity community should continue to engage with the operational *technology community to promote awareness and accelerate cybersecurity technology transfer.*

In the past, most operational technology relied on stand-alone networks. Now, more and more control systems are being connected to the Internet, requiring that the operational technology community learn about new tools and techniques. This will not be a fast process, so Cloudflare is glad to see these challenges highlighted in the draft report.

Goal 5: Increase awareness and education across the ecosystem

Goal 5 is important not only because it can help in the fight against botnets but because efforts in this area can help improve the security of both the Internet of Things and IT infrastructure around the world. The Federal government has a unique and critical role to play in funding education (and curriculum development) in computer science and engineering (at both the university and K-12 levels).

Action	**Benefit**	**Difficulty**	**Time**	**Impact**
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 will intuitively trust and understand.	Med.	Med.	Med.	Narrow
Action 5.2 The private sector should establish a 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.	Med.	Med.	Med.	Med.
Action 5.3 Government should encourage the academic and training sectors to fully integrate secure coding practices into computer science and related programs.	Med.	High	Long	Broad
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.	Med.	High	Long	Broad
Action 5.5 The federal government should establish a public awareness campaign to support recognition and adoption of the home IoT device security profile and branding.	Med.	High	Short	Narrow

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 will intuitively trust and understand.

This effort would provide benefits far beyond DDoS mitigation. Governments have played a critical role in promoting everything from toy safety to drug abuse prevention to safe driving. The challenge with encouraging consumers to buy more secure IoT devices is that the potential harms are harder to describe and visualize and the consumer can often save money by buying the cheaper, less secure device.
Action 5.2 The private sector should establish a 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.

Like Action 5.1, this effort would provide benefits far beyond DDoS mitigation. Independent, government-initiated rating systems have played an important role in automobile safety, energy efficiency, and other areas. But, as noted in the draft report, IoT devices are incredibly varied and evolve rapidly, so consumer rankings and cybersecurity assessments will have a hard time keeping up with the market. Still, having trusted labels that consumers could use to determine if the device they are thinking about buying has fundamental security flaws could reduce the number of devices that could be exploited for the next Mirai-type botnet attack. It could also encourage equipment vendors to adopt secure gateways or other edge-based services to protect their devices.

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

Of all the recommendations in the report, this is the one that could have the broadest positive impact beyond the rather narrow problem of DDoS mitigation. It is clearly needed. In too many universities, it is possible to get a computer science or computer engineering degree without taking a cybersecurity course. And many students are investing time and dollars in cybersecurity degrees or training programs that are too narrow and do not teach them the skills needed to be an all-purpose developer or to keep up with a rapidly-evolving field. As a company that employs more than a hundred engineers (and will be hiring hundreds more in the near future), Cloudflare supports anything that will train more well-rounded computer professionals with a deep understanding of cybersecurity.

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.

This is an even more ambitious proposal than Action 5.3 and is certain to take even longer. But, particularly as every sector of the economy becomes digital, it is critical that all types of engineers understand how the systems they design and run could be subject to cyber attacks--and what they could do to counter them.

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

This proposal ties in with Action 5.2 on a voluntary labeling program for IoT devices. Again, we stress that any effort to evaluate the security of IoT devices not merely look at the device but also look at how it will be connected to the Internet and whether that will be done in a secure way that both protects the devices and protects the rest of the Internet from botnet traffic should the device be compromised.

Next Steps

Cloudflare has been very impressed with the open, transparent way in which this report has been drafted, as well as the willingness of the the teams at the Department of Commerce and the Department of Homeland Security to incorporate new ideas into their work. We participated in last year’s workshop at NIST and look forward to participating in the NIST workshop on the draft report scheduled for February 28 and March 1. We look forward to the final report and will work to help ensure that its recommendations are implemented and not ignored.