To: The Department of Commerce Internet Policy Task Force
From: Messaging Anti-Abuse Working Group (MAAWG)
Date: July 29th, 2011
Subject: Comments on "Cybersecurity, Innovation and the Internet Economy"

To whom it may concern:

Thank you for the opportunity to comment on the Department of Commerce (DOC) Internet Policy Task Force's seventy-seven page green paper on "Cybersecurity, Innovation and the Internet Economy" (hereafter, "the report"), as was publicly made available at http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf

The Messaging Anti-Abuse Working Group (MAAWG) is an international non-profit industry-led organization founded to fight online abuse such as phishing, botnets, fraud, spam, viruses and denial-of service attacks. MAAWG draws technical experts, researchers and policy specialists from a broad base of Internet Service Providers and Network Operators representing over one billion mailboxes, and from key technology providers, academia and volume sender organizations. The multi-disciplinary approach at MAAWG (http://www.maawg.org/) includes education, advice on public policy and legislation, development of industry best practices, guidance in the development of industry standards and the facilitation of global collaboration.

This document will address a number of areas and topics raised in your report, with our comments generally following the order in which topics were introduced there.

In the following comments, all "section" references refer to the various sections of the Task Force's report. For example, the following section, labeled "Section II," is providing comments on Section II of the Task Force's report. All page references in the following comments are to the PDF page numbers associated with the electronic version of the report.

Section II. The Report's Definition of the "Internet and Information Innovation Sector ("I3S")

We note on PDF page 21 that you would like input on

> *How should the Internet and Information Innovation Sector be defined? What kind of entities should be included or excluded? How can its functions be clearly distinguished from critical infrastructure?*

Response: MAAWG believes that the Department of Commerce should not attempt to artificially create a new "Internet and Information Innovation Sector" (I3S). The entities that have been vaguely described as targeted for inclusion do not constitute a coherent community of interest, and attempting to force a union where no natural basis for such a union exists would be ill considered. If the I3S does not get "created" by the Department, the question of what entities should be included or excluded, and how its functions can be distinguished from those involving critical infrastructure, become moot.

If the DOC *does* determine that it should proceed to establish the I3S, MAAWG urges the administration to employ a narrow definition of what constitutes "critical infrastructure," excluding "information systems" and "information technology" from its definition moving forward. See the discussion below, beginning on page 3, for more on this important point.

Discussion: Federal responsibilities for cybersecurity continue to evolve, and we agree with the Internet Policy Task Force that an important part of its remit is, and should be, articulating the bounds of its cybersecurity role vis-à-vis other Federal agencies, the business sector, the public and other nations and business entities abroad. For example, as you note on PDF page 18 of the report, the Department of Homeland Security (DHS) has primary responsibility for working with private and public sector stakeholders to protect our nation's Critical Infrastructure and Key Resource (CIKR), and that the White House' Cybersecurity Coordinator is "responsible for setting a national agenda and for coordinating Executive Branch cybersecurity activities." Clearly, the Department of Commerce (DOC) has no interest in contending for managerial authority over the nation's cyber CIKR nor do you wish to become the Executive Branch's cybersecurity oversight and management agency. This is as it should be.

This is not to say that the DOC has no role whatsoever when it comes to cybersecurity. As noted in the report, the National Institute of Standards Technology (NIST), a DOC unit, does play an appreciated role in developing "standards and guides for securing non-national security federal information systems," and the National Telecommunications and Information Administration (NTIA), another DOC unit, acts as "principal adviser to the President on telecommunications and information policies," having "worked closely with other parts of government on broadband deployment, Internet policy development, securing the Internet domain name space, and other issues." Thank you for your work in these important areas.

However, section II of the report, beginning on PDF page 20, seeks to establish a new role for the DOC, in part by defining an odd new entity the report elects to call the "Internet and Information Innovation Sector" or "I3S."

That entity is defined in the report:

> *This business sector includes functions and services that fall outside the classification of covered critical infrastructure, create or utilize the Internet and have a large potential for growth, entrepreneurship, and vitalization of the economy. More specifically, the following functions and services are included in the I3S:*
>
> - *provision of information services and content;*
> - *facilitation of the wide variety of transactional services available through the Internet as an intermediary;*
> - *storage and hosting of publicly accessible content; and*
> - *support of users' access to content or transaction activities, including, but not limited to application, browser, social network, and search providers.*

What a curious hodge-podge of disparate elements to try to combine into this new I3S entity.

As we're sure you're already aware, the constituent parts of the Internet ecosystem do not self-aggregate or self-organize themselves this way. The community of interest you purport to describe simply doesn't exist, and some parties mentioned in the quoted paragraph have perspectives and interests that are diametrically opposed to those of other stakeholders with whom they've been unilaterally combined.

On PDF page 20 of the report, the report mentions worries from some commentators that non-harmonized cybersecurity policies might potentially "balkanize the cybersecurity and associated legal landscape." We're struck by that metaphor, if not by its underlying premise (with which we disagree).

In fact, we believe that the DOC's attempt to create this new "I3S," in a putative effort to avoid "balkanization" would actually result in the establishment of a dysfunctional "online Yugoslavia." By this we mean that you are attempting to artificially combine fundamentally immiscible elements with all the inevitable problems associated with such an ill-fated effort.

We do understand that having a single composite entity would be administratively convenient (at least in so far it provides a short hand name by which the DOC can essentially refer to "all parts of the Internet industry that are not already subject to another agency's cybersecurity oversight"), but attempting to create a federation in anything other than name where no organic basis for one exists is an undertaking doomed to failure.

We urge the DOC to abandon its attempt to promulgate the notion of an "I3S." We would suggest, instead, that the DOC recognize and refer to well-established and well-understood Internet industry segments (such as "Internet Service Providers") by their routinely employed names, instead. Everyone knows and understands what an "ISP" is, even if they've never heard of "I3S."

The Question of What Should Be Included In "Critical Infrastructure."

The question of what should be considered to be "critical infrastructure" is pivotal to determining whether cybersecurity for a given industry segment is the responsibility of the Department of Homeland Security, some other agency (such as potentially the Department of Commerce), or something that should be left to the judgment of each individual company in that segment.

It may surprise some to learn that what is (or isn't) critical infrastructure isn't something that's completely settled. Most would assume, paraphrasing Mr. Justice Stewart's famous remark from his concurring opinion in Jacobellis v. Ohio[1] that when it comes to critical infrastructure, just as in some other things, "we know it when we see it."

For example, if you were to ask average Americans to describe some examples of "critical infrastructure," their responses would surely include things such as the national power grid and key energy pipelines, dams, major airports, chemical plants and refineries, etc.

No one would disagree that those facilities are part of our nation's "critical infrastructure."

However, you might be surprised to learn that the definition of what's "critical infrastructure" has fluctuated and evolved over time. In 2004, the Library of Congress Congressional Research Service did an entire study that was devoted to just examining the evolution of the term "critical infrastructure" over a period of some 20 years.[2]

"Information systems" or "information technology" has been formally included in the definition of the term "critical infrastructure" since 1998, and "telecommunications" has been part of "critical infrastructure" since at least 1996. Some, such as Theodore Gyle Lewis, go so far as to asset that

---

[1] Jacobellis v. Ohio, 378 U.S. 184 (1964).

[2] "Critical Infrastructure and Key Assets: Definition and Identification," CRS Report for Congress RL32631, October 1st, 2004. http://www.fas.org/sgp/crs/RL32631.pdf

telecommunications was the earliest "critical infrastructure," dating to the telecommunication failures of the Cuban Missile Crisis in 1962.[3]

The Department of Homeland Security also makes it clear that from their point of view, "information technology" remains a key part of "critical infrastructure." According to DHS, the Information Technology sector plays a role which is...

> *central to the nation's security, economy, and public health and safety. Businesses, governments, academia, and private citizens are increasingly dependent upon IT Sector functions. These virtual and distributed functions produce and provide hardware, software, and IT systems and services, and -- in collaboration with the Communication Sector -- the Internet.*[4]

That inclusive definition aside, however, we'd ask that the administration apply a "common sense test" when it comes to what is and isn't "critical infrastructure."

When we're talking about true critical infrastructure, its failure is always something that can hurt or kill people. True critical infrastructure can be said to always be "life-safety critical."

For example, if air traffic control fails, planes may collide in flight, or crash while trying to land. If the power grid fails in winter, families may freeze to death. If hydropower facilities are attacked, flooding may inundate homes and businesses, or sweep people downstream to their deaths. *Those* are examples of our country's true "critical infrastructure," and examples of well-defined activities that need to be carefully protected from terrorist attacks.

On the other hand, while we might like to think that we'll "die" if we cannot read our email, surf the web, or post an update to our favorite social networking site, trust us on this, in reality, the consequences of such an outage will not be so irrevocably dire.

The world will go on, even if we can't Tweet or send an IM. We may be irritated or inconvenienced if we can't use the Internet, but we won't be laying burning in the wreckage of an airplane, nor will we freeze to death or drown.

Enterprise "information systems" and "information technology," including the Internet, are unquestionably *important*, but when all is said and done, they do NOT meet the "common sense" test we advocate as the standard for something to be considered truly "critical infrastructure."

Trying to treat them as if they are "critical infrastructure" diverts limited resources from being used to protect the true critical infrastructure that really is being targeted for attack by terrorists and others who would do the nation harm. Al Qaeda is *NOT* trying to "take down the web," if only because they, too,

---

[3] Theodore Gyle Lewis, "Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation," Wiley-Interscience, 2006, SBN-13 978-0471786283 at pages 3 and 30-31.

[4] "National Infrastructure Protection Plan: Information Technology Sector," Department of Homeland Security. Undated. http://www.dhs.gov/xlibrary/assets/nipp_snapshot_informationtechnology.pdf (linked from http://www.dhs.gov/files/programs/gc_1188479464996.shtm)

find it convenient to use (albeit for their own nefarious purposes).

Moreover, unlike a chemical plant, dam, air traffic control center, or power generation facility, can we even point to "information systems" or "information technology" and say, "Here. This is it. Protect these facilities?" No. Information technology, and information systems, and the Internet in general, are everywhere these days. It is highly decentralized and distributed, and as such, it would be impossible to protect information systems or information technology or the Internet the same way we might true critical infrastructure.

We will concede that process control systems (such as the networks that are used to operate chemical plants), and SCADA systems (as are used to operate distributed infrastructure such as petroleum pipelines), *are* "critical infrastructure." Those systems and networks, separate from the Internet (at least when all is architected as it should be), *can* be clearly delineated and, if attacked, *could* very well cause serious injuries or fatalities. As such, process control systems and SCADA systems SHOULD be protected as critical infrastructure. We urge you to note, however, that this is a very narrow exception to the general rule that "information systems" or "information technology," while important, are NOT strictly speaking "critical infrastructure."

Other Section II Questions/Comments.

A. Beyond proposing the creation of the I3S, the Task Force had other specific questions in Section II, such as on PDF page 20. Specifically, the Task Force asked:

> "Is Commerce's focus on an Internet and Information Innovation Sector the right one to target the most serious cybersecurity threats to the Nation's economic and social well-being related to non-critical infrastructure?"

Response: As mentioned in the preceding section, we do not believe that the DOC needs to create an artificial "sector" to target the serious cyber security threats we collectively face, nor does it need to create additional legislation or regulations or "codes of conduct," etc. The administration already has plenty of authority to improve U.S. cybersecurity if agencies would just exercise their existing powers.

Discussion: For example, MAAWG remains exceptionally concerned about the state of "dot com" domain names, and other gTLD domain names, as administered by the Internet Corporation for Assigned Names and Numbers (ICANN) under an agreement with the Department of Commerce. The Department does not need new authority to deal with domain name issues and ICANN, it simply needs to exercise the authority it already possesses pursuant to its existing agreement with ICANN.

Let's consider a specific example: domain name whois data accuracy. Domain name whois data is supposed to record the name and contact information associated with those controlling a domain name. Service providers, law enforcement officers, private investigators providing civil litigation support, companies considering entering into an online transaction, and many other entities should be able to rely on domain whois data when it comes to "knowing who's behind" a given dot com (or other gTLD) domain.

Unfortunately, because of lax oversight from DOC, the state of whois data is all too often simply farcical, bearing no relationship whatsoever to reality. Whois data may be missing, full of gibberish, or contain mocking elements reflective of a widespread popular belief that anything -- anything at all -- can

be entered because "no one's going to check" and "no one actually cares."

Registrars, who should be responsible for the whois information they allow their customers to submit, aren't held accountable. ICANN routinely receives end-user reports of whois inaccuracies via the WDPRS process,[5] yet even the worst registrars (such as so-called "bullet proof" registrars allowing the most egregious misconduct) are never deaccredited/terminated.

Things as simple as even basic internal address consistency checks, checks that are routinely done as an anti-fraud step by the private sector, don't take place when ICANN allows a domain registration to occur. As a result, domain whois data has degenerated into an untrustworthy and inaccurate swamp. Why? Because the DOC has not employed its existing authority when it comes to overseeing ICANN-contracted operations. Why should Commerce be delegated *further* cybersecurity authorities, if it isn't discharging its *current* responsibilities?

For that matter, we find it inconceivable that the Department of Commerce would turn a deaf ear to the ongoing efforts of the federal law enforcement community to fix ICANN-related issues such as unusable whois data. Surely professional comity would imply some willingness to investigate and address the issues that brother Federal agencies are struggling to resolve!

B. On PDF page 20 you also asked:

> *What are the most serious cybersecurity threats facing the I3S as currently defined?*

Response: The list of serious potential cybersecurity threats is very long, and includes both technical and administrative issues. To name just a dozen by way of example:

- Spam (including email spam, SMS spam, web page spam, etc.)
- Malware (such as viruses, worms, trojan horses, root kits, spyware, etc.)
- Attacks against authentication infrastructure, including both attacks against traditional password-based authentication systems and attacks targeting two factor solutions
- Vulnerable web applications (cross site scripting, SQL injection, etc.)
- Distributed denial of service (DDoS) attacks
- Poor physical security of networks, servers and other enterprise cyber infrastructure, including with respect to low-probability (but potentially national-scale) cyber risks
- Insecure wireless networks, used in insecure ways
- Inadequate personnel vetting and controls (aka "the insider threat")
- Breaches involving personally identifiable information (PII) and other privacy failures
- Diversion of resources/preoccupation of staff with non-operational security "compliance" responsibilities, resulting in the hiring of lawyers and auditors rather than technical security staff (or well trained system administrators and network engineers)
- Loss of technical functionality as a result of overreaction or inappropriate responses to cyber vulnerabilities (extremely tight firewall policies may make it difficult or impossible for staff to get their substantive work done)
- Untrustworthy hardware (such as cloned "grey market" routers or router interface modules, or internationally-sourced microelectronic chips of unknown provenance)

---

[5] http://wdprs.internic.net/

Discussion: While that list isn't offered in any particular order, we didn't err by beginning that list of serious cyber threats by mentioning spam. We know that it may surprise some readers. You may not think that spam is still a serious cyber security threat -- after all you may not see much of it in your inboxes any more.

Please don't be misled.

Spam continues to be a major concern for MAAWG's membership, and dealing with spam via technical means -- so that you *don't* see spam in your inbox -- costs the industry many millions of dollars a year. We'll also admit that while we all do our best to avoid any potential "false positives," we know that when filtering spam, we will likely also accidentally block some legitimate and wanted email. These false positives, while normally quite rare, are another very real "cost" associated with filtering spam that we must never forget. Spam is also the foundation technology that enables many other cyber ills such as phishing and the distribution of malware. No, clearly, spam remains a major cyber security threat, and one that deserves more attention from the government than it currently receives.

As an example of how we need more use of existing laws rather than the creation of many new ones, note that existing legislation already allows the FTC to prosecute spammers. The laws we need largely already exist.

But, how many major CAN-SPAM cases has the DOC's enforcement partner, the FTC, undertaken in the last few years? Anti-spam laws exist, but if they don't lead to investigations, prosecutions, convictions, and serious penalties, those laws effectively mean little.

Simply passing more laws or writing additional regulations will not mean anything unless agencies are motivated to go after spammers, something that's currently apparently an abysmally low agency executive priority. That's a shame, since in many cases:

- We know who these spammers are (see, for example, the Spamhaus Register of Known Spam Operations)[6]

- We know where these spammers live and work -- many of them are based in the United States, where they are easily subject to US law enforcement and regulatory enforcement action.

- The FTC has very technically talented and hardworking investigators and attorneys who could easily investigate and litigate many major spam cases every year, but the FTC's executive management has failed to authorize them to do so.

Executive management at the FTC needs to make prosecuting spammers a top agency priority, and they need to begin tracking the successful execution of those priorities by establishing concrete milestones with measurable annual numeric target goals. An example of such a goal might hypothetically be "Successfully prosecute three dozen major American spammers during calendar year 2012."

Alternatively, perhaps Congress should charge a different agency (such as the Department of Commerce?) with responsibility for civil investigation and prosecution of spammers.

---

[6] http://www.spamhaus.org/rokso/

If we can't make progress against as "simple" a cybersecurity problem as spam, what chance do we have when it comes to dealing with some of the unquestionably "complex" cybersecurity problems out there?

Section III-A-1 "Developing and Promoting I3S-Specific Voluntary Codes of Conduct"

A. In this section, you commented:

> *In the I3S, firms often lack a mechanism for establishing common cybersecurity practices, promoting widely accepted standards or undertaking other cooperative action against specific threats in this area. Where coordination has happened, it has mostly been by volunteers and advocates through newly created groups such as the Messaging Anti-Abuse Working Group (MAAWG) [...]*

MAAWG, now seven years old and having just held its 22nd general meeting, appreciates your recognition of our efforts to improve operational cybersecurity. Thank you!

B. *The Importance of Voluntary International Efforts:* On PDF page 22 in the report, you mention that

> *Several of the comments received from the NOI process stressed the use of voluntary efforts as the best means to create principles and guidelines for promoting cybersecurity among what are essentially parts of the I3S. [footnote 13]*

If one checks footnote 13 in the report, one can see that MAAWG was one of those offering comments to that effect. We reiterate our support for that important point today.

C. The foundation that voluntary industry efforts provide, however, should <u>not</u> be abused as a sort of "closet rulemaking" process which will eventually results in the industry being subject to enforceable compliance requirements, as proposed later on that same page:

> *Once these codes have been developed and companies have committed to follow them, relevant law enforcement agencies, such as Federal Trade Commission (FTC) and State Attorneys General, could enforce them, eventually leading to norms of behavior promoting trust in the consumer marketplace.*

Response: MAAWG opposes that strategy.

Discussion: There's no surer way to quash industry interest in a voluntary standards development process than to introduce the specter that those "voluntary" practices may someday be "used against us" by being turned into enforceable regulations. Don't quash industry's interest in making progress, or its freedom to experiment, innovate and resolve the problems it faces, by threatening to turn voluntary industry standards into mandatory government requirements.

As you consider that recommendation, two additional factors to keep in mind include:

- Not all entities may need, or be equally ready to adopt, industry recommended principles and guidelines for promoting cybersecurity, and

- Not all principles and guidelines may be equally applicable to all market participants. What might work well for a large bank, might be a disaster for a social media company.

A free market approach, guided by industry recommendations, will allow ISPs (and other members of what the report refers to as the "I3S") to devote their best efforts toward focusing on improving actual *operational security* rather than on meeting paper-based *compliance reporting* requirements.

Many times, if new security innovations didn't get adopted, it hasn't been because there wasn't an interest in doing so, it has simply been that there was no money to do so in these difficult economic times. If the administration views cybersecurity as a priority, as we believe it does and should, we would encourage the administration to provide funding for worthy operational cybersecurity initiatives it might like to promote, rather than passing and imposing new unfunded cybersecurity mandates. We welcome government ideas and participation in improving cybersecurity, but please back those new ideas up with financial support, don't just drop additional economic burdens on already struggling businesses.

We'd also note that talking about having the FTC and state attorneys general enforce what were once voluntary codes of conduct perhaps reflects insufficient appreciation for the global scope of the cybersecurity problems we face. The FTC has limited authority to regulate businesses abroad, and obviously state attorneys general have an even more limited geographic scope, yet cybercrime is not something that's limited to just to the United States (or any subset of states thereof). Solutions to our cyber security issues require us to work collaboratively with our non-US members, and with international regulators and international law enforcement agencies, and success in that work requires collaboration and persuasion, not coercion.

D. *Government Participation In Developing Voluntary Codes of Conduct:* PDF page 23 includes the observation that *"A key role for government is to assist industry in developing these voluntary codes of conduct*."

MAAWG has an established track record of inviting participation from relevant trusted third parties, including international and domestic government technical experts, cyber regulators, and law enforcement officers committed to fighting messaging abuse. We value and appreciate their ongoing insights and contributions, and we consider them "part of the MAAWG family," helping us to fight messaging abuse and to improve operational security.

However, a close reading of the quoted comment from PDF page 23, as well as the language of Policy Recommendation A1, leads us to believe that the Department envisions a new role, one where it is the convener/facilitator (rather than a participant on an equal footing with industry, non-governmental organizations, technical experts, and international participants).

Response: MAAWG opposes that refactorization.

Discussion: Existing organizations, including MAAWG itself, are successfully generating guidance for industry participants, and allow for government participation and input. We're already "work[ing] internationally to advance codes of conduct in ways that are consistent with and/or influence global norms and practices," as the Policy Task Force urged in Policy Recommendation A1. Given those realities, we believe that the DOC should not attempt to "rediscover" or "recreate" that which already exists. Join us and work with us, don't try to "clone us" as part of some agency activity.

We do recognize that international participation can be difficult/expensive. While MAAWG routinely holds at least one meeting a year in Europe, MAAWG has not held meetings in Asia or in the southern hemisphere.

If the administration would like to facilitate a wider geographic sphere of influence for MAAWG or other industry cyber security-focused organizations, one option would be for the DOC, or the State Department, or another federal agency to provide grant funding helping to underwrite the costs that would be associated with undertaking an expanded program of international meetings and collaboration.

Section III-A-2. A. "*Promoting Existing Keystone Standards and Practices:*" At the bottom of PDF page 24 and continuing onto page 25, the DOC describes its intent to promote "existing keystone standards and practices." Again, we quote:

> *It is clear that the government should not be in the business of picking technology winners and losers; however, where consensus emerges that a particular standard or practice will markedly improve the Nation's collective security, the government should consider more proactively promoting industry-led efforts and widely accepted standards and practices and calling on entities to implement them. The Department of Commerce plans, consistent with anti-trust laws, to better promote these efforts as a starting point to building better general industry practices.*

The report then goes on to cite a number of potential "baselines" for security implementations, including things like the Payment Card Industry Data Security Standard (PCI-DSS) and NIST 800-53.

Response: While we believe the PCI-DSS and NIST 800-53 have much to offer their respective intended audiences, we do not believe they should be blindly imposed on what the DOC terms the "I3S." Security standards are developed to abate specific risks, and in doing so, they may impose new costs (whether financial, or paid "in kind" as a result of reduced convenience or reduced usability).

Discussion: Attempting to make "one size fit all" would be disastrous. Let us consider one concrete example of this. The PCI-DSS requires enterprises handling payment cards to deploy firewalls. For many businesses, this is fine. However, we know that firewalls can potentially interfere with some applications, such as H.323 video conferencing or peer-to-peer applications or high throughput scientific data transfers. Some firewalls still support IPv6 imperfectly if at all. None of those applications may matter to a site processing payment cards, but any or all of those applications may be critically important to some other type of enterprise, such as a research lab or Internet startup.

B. "*Targeted standards aimed at protecting specific areas:*" PDF page 26 talks about and endorses a variety of specific security technologies, including IPSec, DNSSEC, Internet routing security protocols, web security via SSL/TLS, email security via SPF and DKIM, etc.

Response: We're concerned that the report's authors, or its readers, may mistakenly view these technologies as "magic bullets." They're not.

For example, while DNSSEC can protect against some types of DNS-oriented attacks, it is not a panacea that eliminates all DNS-related risks. Does this mean that we should not promote adoption of DNSSEC? No, obviously not. In fact, when it comes to DNSSEC, MAAWG has offered many sessions about DNSSEC to ensure that its members understand what DNSSEC can -- and *can't* -- do to help them

secure their infrastructure.

DNSSEC has a role, but it is a technology that comes with risks of its own -- for example, industry observers have repeatedly identified (and publicly reported) federal agencies that have had DNSSEC-related misadventures. For example, a major federal agency, having deployed DNSSEC, accidentally allowed its cryptographic keys to expire. When that happened, DNSSEC "worked as architected," and "protected" customers using DNSSEC-validating resolvers by making it impossible for them to reach that agency via the Internet until the agency's DNSSEC cryptographic keys had been properly updated.

Or consider attempting to enhance web security with SSL/TLS. SSL/TLS protocols are meant to achieve *three* objectives: protecting traffic from eavesdropping, protecting traffic from tampering, and protecting users from inadvertently trusting fake websites (rather the entity they'd really meant to reach).

Regretably, a "race to the bottom" in the "domain validated" (DV) certificate market means that users of most SSL/TLS-"secured" web sites have no idea whom they may be dealing since pre-issuance identity validation checks have disappeared.

These days, all the certificate authority does before issuing a DV certificate is verify that the person requesting the DV certificate can read mail sent to one of several published domain contact addresses. That doesn't even begin to provide genuine "identity" validation.

SSL/TLS-enabled web servers can also be part of the problem, and may only provide an illusion or appearance of security if they aren't correctly configured, even if they do use a broadly accepted SSL/TLS server certificate.

As an experiment, test a publicly accessible "secure" web site of your choice using the publicly available Qualys SSL Labs SSL Server Test page.[7] We suspect that you may be surprised, as we were, at the number of "secure" web servers that support insecure and obsolete versions of the SSL protocol, that accept weak cipher suites, or that are vulnerable to insecure renegotiation.

Thus, simply saying, "You should be doing SSL/TLS" isn't enough. As mathematicians would say, "it's necessary, but not sufficient." We're happy to see the report itself render the same opinion, noting on PDF page 26 that

> *It is important to note that while implementation of these guidelines or standards may be necessary to protect security in certain instances, they are almost never sufficient when implemented in isolation. Moreover, particular standards may harden information systems from particular avenues of attack, but may leave other avenues open.*

This is very true, and very important for everyone to note. We urge you to emphasize this point further.

We are also concerned that the report is promoting some security technologies that are currently very immature and not very broadly adopted at all. For example, efforts to improve Internet Routing Security are really just in their seminal phase, and the solutions that are currently being experimented with, such as rPKI, may be too new too be adopted for routine production use by some carriers.

---

[7] https://www.ssllabs.com/ssldb/index.html

We would also urge the administration to lead by example when it comes to promoting technical security solutions it believes in, and which it believes the industry as a whole should be using. Currently, the federal government often does not do so. If you would have us "do as you ask," please, first, "do yourselves as you'd have us do." Put another way, "lead by example, not by fiat."

For instance, are all federal agencies using DKIM and/or SPF, as the report recommends on PDF page 26? No, they're not. That's the sort of disconnect between "what the government says" and "what the government actually does" that undercuts the credibility and authority of this and other technical federal cybersecurity recommendations.

Section III-A-3. "*Promoting Automation of Security:*" Beginning on the bottom of PDF page 27 and continuing onto PDF page 28, the report discusses the value of automating security-related tasks.

Response: We agree that improving automation of tasks such as operating system and application patching, is very important, and currently often imperfectly performed. Encouraging use of security automation here in the United States is not a complete solution, however.

Many of the systems that go unpatched -- and which ultimately get compromised and turned into spam-spewing bots (or abused in other ways) -- are overseas in thinly connected areas of the world. In those remote locations, it may take hours or days for a user to download the patches for a single application, if it is possible at all (and in the third world, many applications may be pirated and hence not eligible for vendor patches and support, thereby ensuring that that it is just a matter of time until they get exploited if they weren't shipped already trojan'd "out of the box"). We need a strategy to address this pressing issue.

This section also discussed the National Vulnerability Database (NVD). We would like to take this opportunity to express our support and to endorse that excellent project.

We also support and encourage the government's use of "procurement strategies" to encourage the market to field innovative security solutions. The procurement "hammer" you wield is indeed influential. You are a very large and important customer for virtually all security companies, and that position means that when you demand support for a particular technical security solution, you will get it, and because you get it, that solution will also be available for the commercial marketplace.

MAAWG therefore supports policy recommendation A3 on PDF page 29 *("The U.S. government should promote and accelerate both public and private sector efforts to research, develop and implement automated security and compliance.")*

In your work to promote security automation, though, we urge you to recognize that automation can be something of a two-edged sword.

While automation can simplify and improve our ability to keep systems up to date, automation can also make it possible for us to drown us in irrelevant minutiae. Consider intrusion detection systems and log analysis systems, for example. If security analysts are inundated with "false positives" or veritable drifts of informational alerts, we may miss critical high priority events. Automation needs to not just give us a more complete and more accurate view of the world, it needs to help us avoid information overload. This is the sort of task that automation can potentially excel at, if we make it a development priority.

We'd also like to note that it would be important for human analysts to continue to be able to access raw data, and to be able to manually review both "hits" and "non-hits" that automated systems may have identified. Our security is made worse if deployment of automation means that security analysts lose a "feel" for the data that's being analyzed, or analysts blindly trust automated processing systems without the ability and obligation to do periodic "quality control" checks.

Section III-A-4: "*Improving and Modernizing Security Assurance:*" Beginning on PDF page 29, this section talks about what security assurance standards the United States should adopt or promote.

Response: We concur with the caution from PayPal, mentioned on PDF page 30, that rigid certification standards can lead to delayed deployments; we'd go so far as to say that rigid certification requirements, particularly when technology is also import/export controlled, can result in limited market options.

Discussion: A fine example of this would be PKI hardware security tokens, meant to securely store X.509 personal certificates per FIPS 140-2. Because of the stringent requirements associated with getting such a token design certified, as well as international cryptography export controls, the net result is that there are few options for procuring these critical devices here in the United States, and personal certificates have rarely been deployed, with only a few notable exceptions such as the Federal Common Access Card program.

Tying this in with messaging security (MAAWG's primary focus), this means that use of S/MIME for message signing and encryption is seldom seen in this country. PGP (or GNU PrivacyGuard) has come to dominate the *ad hoc* messaging signing and encryption market, but that means that encryption and signing of all sorts is less common than it should be in the enterprise market: a lack of affordable hardware tokens discourage S/MIME, and PGP has an awkward trust model for enterprise deployment.

Thus, when federal policy decisions relating to security assurance are made, full consideration needs to be given to the fact that setting a "hard-to-reach bar" *may* result in highly secure products, but may also result in potentially few market choices.

Stringent assurance requirements can also mean that even when choices are available, prices may be unacceptably high due to the need to recoup burdensome assurance-related costs.

Thus, carefully vetted high cost products from a limited number of domestic vendors may, ironically, provide an exploitable opportunity for some of our most sophisticated cyber opponents abroad. If an institution here in the United States cannot get the certified products they need (at a price they can afford) from a trustworthy domestic vendor, they may turn to low-cost (but less-trustworthy) third-world sources for critical security hardware (such as the PKI hardware security tokens we mentioned). If this were to occur, it would be a prime example of how well meaning stringent security assurances might paradoxically result in potentially far-less-secure ultimate outcomes.

One way to help avoid this would be by improving commercial access, by Americans, to trustworthy EU-origin strong cryptographic products. While US users might assume that they'd have ready access to all strong cryptographic products produced in Europe, at times we may not. Just like Sudanese or North Koreans trying to buy cryptographic products from the US, American users may be surprised to find that some EU suppliers of strong cryptographic hardware do not have permission from the EU to export their products to the United States, something that most Americans would find unpleasantly surprising.

The administration should insure that US users are able to freely buy strong cryptographic hardware from trustworthy suppliers in the European Union, should they desire to do so, and reciprocally, EU users should have ready access to US strong crypto hardware solutions.

We also note that certification processes can make innovation lag market technology developments.

Continuing with the example of hardware PKI tokens used to securely hold personal certificates, most hardware PKI tokens have a USB format, and plug into laptops via an open USB port. But where are the affordable solutions for mobile devices that may not have a USB slot? So-called "CAC sleds" allow a federal CAC card to communicate with a mobile device via secure Bluetooth, but CAC sleds are marketed (and priced) for a limited federal market, not for mass-market adoption.

Assured security technologies need to be nimble enough to keep pace with the rapid innovation that characterizes today's Internet, including things like "slick-sided" mobile devices with limited physical interconnection options and relatively low acceptable consumer price points.

Section III-B-1. *Developing incentives to promote adoption of cybersecurity best practices*.

On PDF pages 32-37 of the report, the Task Force discusses incentives meant to promote adoption of cybersecurity best practices, ultimately summarizing that discussion with Policy Recommendation B1:

> *The Department of Commerce and industry should continue to explore and identify incentives to encourage I3S to adopt voluntary cybersecurity best practices*.

MAAWG supports Policy Recommendation B1, subject to the concerns previously outlined.

Section III-B-2. *Using security disclosures as an incentive*.

A. This section of the Task Force's report begins with the remark:

> *In its Green Paper on commercial data privacy, the Task Force endorsed the adoption of transparency and disclosure of information practices as an important measure*.

And then went on to quote MAAWG's earlier comments on this topic later in this section:

> *MAAWG stressed that the best cybersecurity incentive is for government to "increase transparency and accuracy with respect to the Internet names and numbers it oversees," which would allow the community to "make informed decisions about their online neighbors."*

We reaffirm that important earlier observation here.

B. *PII and Mandatory Breach Notification Requirements as a "Negative Incentive*." This section of the report lumps the sort of thing MAAWG had in mind (such as requiring transparency from ICANN with respect to domain name registration operations), with a different issue, the mandatory disclosure of data breaches involving PII.

This later topic is a very complex one, and one with potentially profound impacts for both companies

and individuals, yet mandating disclosure is something which is casually described in the report as "a light-handed negative incentive" that "seem[s] to encourage firms to better secure the personal information that they hold about individuals and take steps to prevent the breaches that cause them."

That observation in the Task Force report necessitates comment. No one except cyber criminals wants to see breaches involving PII. Individuals whose data ends up getting breached certainly do not want to have that sort of event occur, but neither does the company which was victimized along with its customers.

A data breach is tremendously disruptive and expensive, with costs including:

- negative publicity,
- costs associated with understanding the attack and technically recovering from it,
- costs associated with notifying and assisting customers (such as with credit monitoring services),
- payment card system fines or fees, or potential loss of ability to accept payment card transactions,
- civil litigation-related expenses,
- loss of customer trust and loss of current and/or future business, sometimes ultimately resulting in complete failure of the business with resulting ripple effects on many innocent parties including "mom and pop" stockholders, employees, suppliers, and the economy as a whole.

Surely no one would pretend that most companies takes the consequences of a potential PII breach casually given those potential impacts. Virtually all companies do the best they can to keep their systems secure,[8] however the bad folk only need to discover one security oversight or one security imperfection to "score," while the good folks need to be near-god-like in their security perfection to "stay safe."

Add to that the fact that in at least some cases, while an intrusion may have occurred, fundamental questions may remain unknown. For example, in some cases it may not be known if PII was even on a lost or stolen system, or, if PII *was* present on hacked system, if that PII was accessed or exfiltrated.

We would thus urge everyone to be careful when it comes to talking about PII breaches and their prevention, because its very easy to go literally overnight from a position of smug self-assurance to being featured on the front page of the newspaper, even when one is trying very hard and doing their very best to keep everything secure.

Bottom line, rather than ruminating about ways to poke at companies when they may already be struggling, we would like to see harsher penalties and more aggressive enforcement against those who intentionally commit crimes involving PII. This would include credit card hackers ("carders") and those who provide goods and services supporting their nefarious activities. We would also like to see improved international cooperation among law enforcement agencies, since, as you know, many of the cyber intrusions that target PII have their origins overseas.

Thus, MAAWG opposes Policy Recommendation B2a.

C. *Public disclosure of security plans and evaluations*. On PDF page 39, the report mentions that

---

[8] We do recognize that on rare occasions there may be some companies that simply aren't trying whatsoever when it comes to protecting the PII that they may hold. If/when that sort of rare situation demonstrably arises, naturally, that sort of "knowing negligence" should be harshly dealt with.

> *The Administration believes that disclosure of cybersecurity plans and evaluations would be an effective tool to promote better security in critical infrastructure. The disclosure of cybersecurity plans and evaluations will allow markets and other firms, the government, and the public at large to hold owners of critical infrastructure accountable for running cybersecurity risks or face liability. We seek additional comment on how such a similar policy tool might be used more expansively within the I3S.*

Disclosure of cybersecurity plans and evaluations might allow the market and others to make an informed assessment of an entity's cyber vulnerabilities, however we believe that in many cases mandatory public disclosures would represent a treasure trove for cracker/hackers.

Rather than having to reconnoiter targets themselves, if mandatory public disclosure were to be required for enterprise security measures, cyber adversaries would simply be able to "look up" a target of potential interest, getting insider-level information about known vulnerabilities and protective measures, presumably involuntarily provided to the government by the company under penalty of perjury.

A hacker/cracker couldn't ask for better assistance than this. Please don't give it to them.

MAAWG opposes any government-compelled public disclosure that might result in company-specific security vulnerabilities being publicly shared with potential adversaries, including opposing Task Force Policy Recommendation B2b.

Section III-B-3. *Facilitating Information Sharing and Other Public/Private Partnerships in the I3S to Improve Cybersecurity.*

On PDF pages 40-42, the Task Force discusses information sharing and public/private partnerships, ultimately concluding, via Policy Recommendation B3:

> *The Department of Commerce should work with other agencies, organizations, and other relevant entities of the I3S to build and/or improve upon existing public-private partnerships that can help promote information sharing.*

MAAWG supports that recommendation, both as a policy recommendation, and as a needs statement underpinning a currently imperfectly met technical security-information sharing capability (sharing security incident information informally, e.g., as PDF reports (in the case of many government security advisories) or as unstructured regular emails, simply doesn't scale beyond certain relatively low limits).

Section III-C-1. *Develop A Better Cost/Benefit Analysis for I3S Security.*

On PDF pages 43-45, the Task Force examines issues related to cost/benefit analysis, and its role in deciding what security investments should rationally be made.

Policy Recommendation C1 states:

> *The Department of Commerce should work across government and with the private sector to build a stronger understanding (at both the firm and at the macro-economic level) of the costs of cyber threats and the benefits of greater security to the I3S.*

MAAWG supports Policy Recommendation C1, provided that any data collection that's done in support of this recommendation is voluntary, and provided that the collecting agency carefully protects any proprietary information that may be shared about threats, countermeasures, and incidents.

Section III-C-2. *Creating and Measuring I3S Cybersecurity Education Efforts.*

On PDF pages 45-48, the report discusses the need for further security education, training, and awareness. The policy recommendation for this part, Policy Recommendation C2, states:

> *The Department of Commerce should support improving online security by working with partners to promote the creation and adoption of formal cybersecurity-oriented curricula in schools. The Department of Commerce should also continue to increase involvement with the private sector to facilitate cybersecurity education and research.*

MAAWG supports Policy Recommendation C2.

Section III-C-3. *Facilitating Research & Development for Deployable Technologies.*

The discussion of this topic on pages 49-53 attempts to summarize comments received about how R&D might facilitate progress on deployable technologies. MAAWG appreciates seeing its earlier comments on this topic mentioned in the summary, including our recommendation that the DOC consider creation of a technical advisory board, and creation of an "X Prize" for “measurable objective achievements in advancing cybersecurity research."

MAAWG is happy to support Policy Recommendation C3, reading:

> *In cooperation with other agencies through the Federal Networking and Information Technology Research and Development (NITRD) framework, the Department of Commerce should begin to specifically promote research and development of technologies that help protect I3S from cyber threats.*

We appreciate NITRD's leadership and efforts in promoting cybersecurity-related research and development, and would appreciate further opportunities to collaborate with and support their work.

Section III-D. *Ensuring Standards and Practices are Global.*

This topic was considered on PDF pages 54-56, and again, we appreciate seeing MAAWG's earlier suggestions referenced and incorporated in multiple places in the Task Force Report's text.

We strongly support Policy Recommendation D1, reading:

> *The U.S. government should continue and increase its international collaboration and cooperation activities to promote cybersecurity policies and standards, research and other efforts that are consistent with and/or influence and improve global norms and practices*

Appendix B. *Widely Recognized Security Standards and Practices*.

A. *IPsec*. In Appendix B on PDF page 69, the report discusses IPsec. Under the paragraph, "Implementation Status," the report discusses deployment of IPsec in both IPv4 and IPv6 networks. As part of that discussion, the report repeats the often heard, but wrong, assertion that IPsec is ubiquitously present in IPv6. As MAAWG technical advisors have discussed in publicly available MAAWG IPv6 training materials,[9] that's incorrect. Adoption of IPv6 and IPsec are essentially orthogonal and unrelated; one can do IPsec without doing IPv6, and doing IPv6 does not presuppose that one will do IPsec.

B. *DNSSEC*. In Appendix B on PDF page 70 and 71, the report discusses DNSSEC. As we previously noted, it is dangerous to zero in on one particular protocol security measure, such as DNSSEC, while failing to consider the full set of issues associated with the underlying protocol (e.g., in this case DNS).

Again, it is MAAWG's pleasure to share advice from one of its technical advisors on DNSSEC and the full suite of DNS-related security considerations that should be considered by sites looking to harden this protocol by potentially deploying DNSSEC or doing other work related to their DNS infrastructure.[10]

C. *Internet Routing Security*. In Appendix B on PDF pages 71-72, the report discusses Internet Routing Security, and correctly notes that most routing security solutions still have limited deployment. We were surprised to see no mention of ARIN's work on rPKI.[11] In the uncertain world of routing security, rPKI is unquestionably the "front-running horse" at this time, and as such should be highlighted.

We also believe that anyone interested in routing security should recognize that substantial value can be obtained now, even if there's still substantial work to be done on many routing security options, simply by monitoring one's own routes, watching for accidental (or malicious) route injections done by unauthorized parties. A variety of options related to this, including some that leverage freely available routing data from the Routeviews Project,[12] are discussed in yet another MAAWG talk.[13]

D. *Web Security*. In Appendix B at pages 72-73, the report discusses use of SSL/TLS to "secure" web sites. Unfortunately, perhaps in an effort to keep the length of the discussion to a reasonable length, the discussion on those pages elides some critical points. For example, on page 73 the report states,

---

[9] Slides 11-19, "MAAWG and IPv6 Security," June 2009, MAAWG Amsterdam, 60 slides. http://pages.uoregon.edu/joe/ipv6_training/maawg-ipv6-security.pdf

[10] "What MAAWG Members Should Know About DNSSEC and The Security of DNS," June 2007, MAAWG Dublin, 60 slides. http://pages.uoregon.edu/joe/maawg10/dnssec-maawg.pdf

[11] https://www.arin.net/resources/rpki.html

[12] http://www.routeviews.org/

[13] "Route Injection and Spam," October 2006, MAAWG Toronto, 80 slides. http://pages.uoregon.edu/joe/maawg8/maawg8.pdf

> *When a SSL certificate is installed on a website, a visitor to that website can be sure that the information entered there is secured and only seen by the organization that owns the website.*

That may be the objective, but there are multiple critical implementation details that may frustrate realization of that goal if the SSL/TLS-enabled server isn't very carefully configured. We don't have room to fully describe all the issues potentially involved here, but a more in-depth discussion of the problem is available for those who may be interested.[14] At a minimum, we urge all web sites relying on SSL/TLS for security to check their site with the free Qualys SSL Labs tester previously mentioned.

E. *Email Security*. In Appendix B at pages 73-74, the report discusses SPF and DKIM. SPF and DKIM are two technologies that MAAWG has spent considerable time discussing, developing and promoting. As such, we perhaps have a more nuanced view of their proper use and intricacies than there was room to include in the Task Force's limited space, or than we have room to include here. We would urge those interested in fully understanding SPF or DKIM to review some of the excellent materials available online, including http://www.openspf.org/ and http://www.dkim.org/ MAAWG is also pleased to offer public access to its DKIM Implementation training videos.[15]

We'd also note that SPF and DKIM are not the only technologies that potentially enhance email security. For example, use of PGP or GNU Privacy Guard is routine in the technical security community for message signing and encryption, and S/MIME is another option for message signing and encryption.

Conclusion

Thank you for this opportunity for MAAWG to comment on the Internet Policy Task Force's excellent report. We know it represents a tremendous amount of hard work on the part of all participants and staff, and even if we cannot agree with some of its recommendations, the professionalism of the Task Force's work when it comes to dealing with a broad and difficult subject is very apparent.

If you would like us to discuss any of our remarks in more depth, or if you have any questions, please do not hesitate to get in touch. We look forward to future opportunities for engagement with the Department of Commerce.

Sincerely,

/signed/

Jerry Upton, Executive Director
Messaging Anti-Abuse Working Group
jerry.upton@maawg.org
http://www.maawg.org

---

[14] "Security and Certificates," June 2011, REN-ISAC Techburst, 80 slides. http://pages.uoregon.edu/joe/techburst/certs-techburst.pdf

[15] " MAAWG DKIM Implementation Training Videos," http://www.maawg.org/activities/training/dkim-video-list