To: National Institute of Standards and Technology –
National Initiative for Cybersecurity Education
From: Messaging Anti-Abuse Working Group (MAAWG)
Date: September 12th, 2011
Subject: Comments on National Initiative for Cybersecurity Education (NICE) Draft Strategic Plan

Please note: *This memo is our preferred submission method because it more clearly outlines our response. However, to aid in your work, we also have incorporated this content into the NIST template.*

To whom it may concern:

Thank you for the opportunity to comment on the National Initiative for Cybersecurity Education (NICE) Draft Strategic Plan dated August 11th, 2011, as was made publicly available at http://csrc.nist.gov/nice/.

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 that can cause great harm to both individuals and national economies. 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.

The NICE Draft Strategic Plan is very well prepared and obviously represents much work from a wide base of contributors. We would like to thank you, and all of your contributors, for your efforts. MAAWG does, however, have some comments on the draft plan that we would like to share with you.

I. The NICE Goals and Particularly the Desire to Raise Public Awareness of Cybersecurity

At lines 64-67, the draft plan states that there are three main NICE goals (subsequently elaborating on those at line 160 and following):

> ***NICE Goals***
>
> *1. Raise awareness among the American public about the risks of online activities.*
> *2. Broaden the pool of skilled workers capable of supporting a cyber-secure nation.*
> *3. Develop and maintain an unrivaled, globally competitive cybersecurity workforce.*

II. Comments on Goal 1

a) Concern You May Be Significantly Underestimating the Difficulty of the Task: While all three of those goals are important, the first goal is of particular interest to us because MAAWG participants

include large consumer ISPs working directly with the public. Like NICE, we all want the American public (and the public in other countries, for that matter) to become more aware of the risks associated with their cybersecurity activities and we particularly want them to take effective steps to stay safe online. However, our fundamental concern is that you may be significantly underestimating the difficulty of the task outlined in Goal 1.

For example, you compare the educational effort required for cybersecurity to the effort required to educate the public about the "hazards of smoking, the wisdom of wearing seatbelts, and the physical benefits of good diet and exercise." [draft lines 214-216] But unlike those challenges, we have not been able to readily distill the cybersecurity message down to a concise message as simple as "don't smoke," "buckle up," or "eat less, eat a balanced diet and exercise every day."

Microsoft, as a case in point, has repeatedly tried to generate a short and effective list of three to five recommendations that, if followed, would allow consumers to operate Microsoft Windows more safely and securely. However if you currently visit http://www.microsoft.com/security/default.aspx, you will see they have shifted much of their emphasis away from user education and are now driving consumers to use automated tools – such as their free antivirus product Security Essentials, their Windows Update that patches vulnerable Microsoft products, and Microsoft Safety Scanner that checks and attempts to fix the user's computer if it becomes infected.

This is a fundamental "sea change" in strategy on Microsoft's part, in our opinion, and one that recognizes some of the unique realities of cybersecurity today:

- Security threats are often subtle and complex and are fully understood only by experts with specialized expertise, expertise the general public typically has neither the background nor inclination to acquire.

- Security threats are continually morphing and evolving, and thus the top cybersecurity threat this month may be obsolete and irrelevant next month. This rapid pace and the dynamic nature of the problem differs significantly from non-cyber threats that may have a more gradual onset and a sustained duration: i.e., campaigns to help the public cope with AIDS, alcoholism, child abuse, drug abuse, heart disease and similar problems do not need to constantly retarget and refocus their efforts.

- Many cybersecurity threats can only be fully mitigated by software or hardware vendor action (e.g., via a vendor issuing updated antivirus signatures or new vendor patches), or by ISPs actively managing network attack traffic. Even if the user wanted to independently tackle some of the cybersecurity threats they face, they may not have the means to do so.

- Users often are confronted by a continual barrage of threat warnings, many of which may not even be relevant to their circumstances. This can be potentially overwhelming for users, particularly those who may not even know what operating system they are using (and thus what alerts apply to them).

- Some users have also grown cynical and jaded, noting that security warnings often are issued from companies selling cybersecurity products. While most cybersecurity companies do a good job of decoupling sales efforts from research notes or white papers discussing new vulnerabilities, the unfounded perception lingers that these disclosures may, at times, be overblown and overstate the true risk users actually face from a given threat.

- Users also face convincing messages from phishers and fake antivirus malware purveyors that confound and confuse them: how do they know which "updates" and "security warnings" they should trust and which ones they should ignore as potential malicious attacks?

b) Educating Users on the Value of the Automated Tools that Keep Systems Secure: Only tightly integrated, automated security tools are ultimately able to address these challenges. To the extent that users simply permit these tools to run, the need for extensive security awareness training may be reduced. If a user cybersecurity awareness campaign theme is to be articulated, the most effective messaging to be conveyed might be that users should not interfere with automated security measures meant to keep their systems secure.

For example, users may perceive automatic updates as excessively time consuming or inconvenient and consequently delay installing them, thereby interfering with the vendor patching process. Another example: users may completely disable a vendor-installed firewall if they believe it might interfere with an application of interest. Others might change browser settings at the urging of particular websites to enable useful (but risky) technologies blocked by default by the browser. These are the types of user behaviors that ultimately undermine scalable automated approaches to improving technical system security, much as users of power tools may sometimes intentionally disable guards installed for their protection.

III. Comments on Goal 2

a) The Need for More Pragmatic Cybersecurity Education: Goal 2, focused on developing and growing our cybersecurity workforce, is also of interest to MAAWG. Most MAAWG member companies employ numerous cybersecurity specialists and no one would dispute that it can be challenging to find technically skilled and affordable staff: the demand is high and the supply is low.

When we delve into the plan's findings, however, at line 309 and beyond cybersecurity is tied to STEM (Science, Technology, Engineering and Mathematics) education efforts. While STEM-related disciplines are important, in truth, most cybersecurity issues have nothing whatsoever to do with biology, chemistry, physics, engineering or mathematics as such. STEM education certainly instills problem-solving skills, but the underlying domain subject matter is often wholly unrelated to cybersecurity workplace needs.

One exception in the STEM approach is, of course, Computer Science. Cybersecurity practitioners certainly benefit from an understanding of computer science topics, but often the emphasis in the courses taught in secondary schools or higher education is generally abstract or theoretical, failing to tackle more pragmatic topics such as:

- Securely configuring and administering large systems and networks
- Using security tools to identify vulnerable hosts and suspicious network attack traffic
- Hardening applications (particularly Web-based applications) to resist focused attacks
- Handling incidents if/when protective measures fail

Curriculums should be adjusted to correct these deficiencies.

Given the global nature of the Internet, it would also be very helpful if more cybersecurity specialists combined proficiency in foreign languages, particularly "Supercritical Need Languages" such as Chinese or other East Asian languages, Arabic or other central Asian languages, etc. Currently our intentional adversaries learn English, but in many cases we do not learn the languages they use. That puts us at a distinct disadvantage. Foreign language skills should be an integral part of cybersecurity curricula, much as foreign language skills were once viewed as a critical tool for scientists.

We also believe there may be insufficient emphasis on "soft skills." This includes working collaboratively with users, verbal and written communication skills, aligning cybersecurity efforts with business drivers, and effectively working with co-workers and management to plan and implement cybersecurity solution strategies.

Unfortunately, there is an ever-increasing government emphasis on regulation and compliance rather than technical cybersecurity. As a result, our greatest cyber workforce need may soon be for more lawyers and auditors specializing in cybersecurity rather than for more technically-focused staff members — although this is a trend we certainly hope does not become more pressing.

b) Create Opportunities for Experiential Education and Data-Driven Research: We would also like to briefly comment on the form that education for the cyber workforce takes.

While classroom education is well established and cost effective, new graduates lacking hands-on practical experience are legion. Nothing substitutes for practical experience, but as we all know, unless you already *have* experience you often do not qualified for a position where you can *gain* experience. We need to break the chicken-and-egg cycle. We urge you to encourage, emphasize and facilitate internships, cooperative educational opportunities, mentoring, the use of adjunct instructors from industry, and other opportunities for students to actually "get their hands dirty" and to understand the practical challenges the industry faces with cybersecurity.

Moving ahead, beginning at line 409, we would like to urge an emphasis on *data-driven* cybersecurity research for graduate-level cybersecurity research and development. What distinguishes scientific scholarship from speculative philosophizing is hard data. In our experience, simulations based on overly simplified models often are substituted for true, hard field data in cybersecurity research. The collection and analysis of actual data is far more likely to lead to valuable insights – and solutions – than simulated data based on simplified abstract models. Cybersecurity inherently involves corner cases, unexpected artifacts and situations that are *not* explicitly well modeled — researchers will only encounter data for these types of events when observing and working on real datasets, and this will require the sort of academic/industry collaboration we have described in these comments.

IV. Comments On Goal 3

Goal 3 is to "Develop and maintain an unrivaled, globally competitive cybersecurity workforce."

When it comes to creating and maintaining the workforce you describe, we note two areas where attention may be needed and where the current plan does not devote sufficient attention:

a) The Federal Security Clearance Model Unduly Constrains the Potential Cybersecurity Workforce: Many cybersecurity positions, particularly in federal government or at federal government contract positions, require more than just domain expertise: a current federal security clearance is also commonly required. Currently there is no process by which an interested and skilled practitioner, albeit one who is not currently a federal employee or federal contractor, can get cleared prior to being hired, even if the applicant is willing to bear the costs of that investigation him or herself.

As a result, the pool of potential applicants for cybersecurity positions requiring a security clearance remains small, growing only when an agency or contractor is willing to "bite the bullet" and hire a particularly promising but uncleared applicant, keeping the employee occupied with non-sensitive make-work tasks until the applicant's clearance can be successfully completed. The clearance process can take months, or even a year or more in some cases, due to the complexity of some investigations and backlogs associated with processing the millions of HSPD-12-related background investigations. We need a program to begin clearing potential cybersecurity specialists before they are offered positions so they can hit the ground running, rather than remaining on the sidelines for months or even longer.

b) An Overemphasis on Formal Certifications May Be Counterproductive: We note that Objective 3.3, at line 575, recommends "Study[ing] the application of professionalization, certification, and licensing standards on cybersecurity career fields."

Earning a certification has substantial value because it forces the applicant to systematically review the body of knowledge covered by a program while also establishing norms of professional behavior in a field where the public may not be able to independently and transparently assess practitioner competence. However, there is a risk that an *overemphasis* on required formal certifications may ultimately be counterproductive.

For example, if having a certificate in-hand is a requirement for performing a particular role, or even being hired, highly qualified candidates who have the required knowledge, but not the necessary credential, may be summarily excluded from consideration. We believe that the *best-qualified* candidate, and not necessarily the most *highly-credentialed* candidate, should always be hired.

This is particularly true if some private cybersecurity certification programs are monetarily expensive to complete, thereby potentially serving as a screening device that might disproportionately impact lower socio-economic-status groups or minorities. While program costs associated with certification programs obviously need to be covered, fee waiver or fee reduction programs should be considered to help the economically disadvantaged participate in what may effectively become "mandatory" certification programs, including both the examinations themselves and any preparatory training that might otherwise serve to "un-level" the credentialing "playing field."

We also note that daunting formal requirements imposed on prospective cybersecurity professionals would limit the pool of potentially available employees. Coupling this constraint with a voracious federal appetite for credentialed cybersecurity professionals, this approach could exacerbate the existing worker shortage as the industry tries to meet its need for cybersecurity talent.

V. Education and Outreach

Section four, at lines 603 and following, focus on education and outreach. A few quick thoughts on this section:

- With respect to conferences, workshops, symposia, etc.: please understand the cybersecurity community already has many events of the sort you envision, to a degree where simply trying to identify an available date when another one could be held without causing material conflicts is difficult. A cybersecurity professional could literally spend the entire year doing nothing but travelling and attending or presenting at major cybersecurity events.

Rather than exacerbating this problem by creating new "must-attend" cybersecurity events, we recommend integrating the activities you envision with one or more of the existing cybersecurity events that are currently broadly attended. If anything, additional value could be generated by underwriting the cost for those who are interested and ready to contribute but lack internal funding to participate in these events.

- While the Internet and the cybersecurity risks associated with it are global, many cybersecurity education and outreach events are not. North American events tend to have North American attendees, European events tend to have European attendees, Asian events tend to have Asian attendees, and so forth, notwithstanding the fact that we all face common transnational cybersecurity threats.

  Given that the Internet makes one's physical location largely irrelevant when it comes to cybersecurity risks, we need to do a better job of integrating cybersecurity professionals worldwide and working together regardless of geographic location. We need the help of our colleagues abroad, and they in turn need us, but in many cases we may not even know each other. (MAAWG has attempted to set an example in this regard by routinely holding one of its three meetings each year in a European venue.)

- We would also like to flag the issue of keeping cybersecurity professionals up-to-date with ongoing operationally-relevant cybersecurity information. By its very nature, many of the aspects that dominate a security professional's day-to-day workload may be too sensitive to publicly share due to the sources and methods that might be exposed by doing so or as a result of other considerations.

  However, if hard-won knowledge that one cybersecurity professional manages to glean is not shared with peers, other professionals may effectively need to "rediscover fire" on their own, time after time. This is true even when what they are (re)discovering is common knowledge among a limited and trusted set of cybersecurity practitioners. This problem is particularly acute for isolated cybersecurity practitioners who work for small firms lacking the budget or critical mass to allow their employees to participate in vetted cybersecurity community activities and become known to, and trusted by, their cybersecurity peers.

  To truly improve the ongoing quality of operational cybersecurity staff expertise, we must tackle the issue of how operationally-relevant sensitive cybersecurity information can be made scalable and securely shared across a large distributed community of cybersecurity practitioners. We do not currently see a clear strategy for meeting this need in the work outlined in section four.

  Related to this, please note that Web-based secure portals often are not effective for sharing because they require an affirmative action by users (logging in and browsing conversation threads) rather than having relevant cybersecurity intelligence automatically "pushed" to security practitioners the way a PGP/GnuPrivacyGuard encrypted mailing list might distribute that same content. If busy professionals need to remember to go hunt for current intelligence in an awkward and inconvenient secure portal, they often simply will not bother.

VI. Conclusion

Thank you for this opportunity for MAAWG to comment on the NICE draft plan. 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 contact us.

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

MAAWG PPC2011-011