To: National Institute of Standards and Technology-National Initiative for Cybersecurity Education
From: Messaging Anti-Abuse Working Group (MAAWG)
Date: September 11th, 2011
Subject: Comments on National Initiative for Cybersecurity Education (NICE) Draft Strategic Plan

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 publicly made 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. 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 a lot of work from a wide base of contributors. We'd like to thank you, and all of your contributors, for your efforts.

MAAWG does, however, have some comments on the draft plan that we'd 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 One

While all three of those goals are important, because MAAWG participants include large consumer ISPs directly working with the public, goal one is of particular interest to us. 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 when it comes to goal one is that you may be significantly underestimating the difficulty of that task.**

Consider, for instance, your comparison of the educational effort required for cybersecurity to the effort required for education about the "hazards of smoking, the wisdom of wearing seatbelts, and the physical benefits of good diet and exercise." [draft at lines 214-216] Unlike those challenges, in the case of cybersecurity, we haven't been able to readily distill the cybersecurity message down to something as simple as "don't smoke," "buckle up," or "eat less; when you do eat, eat a balanced diet; and exercise every day."

Microsoft, for example, has repeatedly tried to come up with a short and effective list of three to five things that, if followed, would allow consumers to operate Microsoft Windows safely and securely. However if you currently visit http://www.microsoft.com/security/default.aspx you'll see that Microsoft has shifted much of their emphasis away from user education toward driving users to run automated tools (such as their free antivirus product, "Security Essentials;" Windows Update, which patch vulnerable Microsoft products; and Microsoft Safety Scanner, which 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 fully understood only by experts with specialized expertise, expertise that 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 differs significantly from non-cyber threat scenarios where risks may have a gradual onset and a sustained duration: 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.
>
> — Users potentially confront a continual barrage of threat warnings, many of which may not even be relevant to their circumstances. This can be overwhelming for users, particularly those who may not even know what operating system they're using (and thus what alerts apply to them).
>
> — Many cybersecurity threats may only be able to 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.
>
> — Some users have also grown cynical and jaded, noting that cyber security warnings often issue from companies selling cyber security products. While most cyber security companies do a good job of decoupling sales efforts from research notes or white papers discussing new vulnerabilities, the unfounded perception lingers that disclose of security vulnerabilities may at times be shrill, and overstate the true risk of users actually being affected by a given threat.
>
> — Users also face convincing messages from phishers and fake anti-virus malware purveyors that confound and confuse them: how do they know what "updates" and "security warnings" they should trust, and which ones they should ignore as potential malicious attacks?

Only tightly integrated automated security tools are ultimately able to address these challenges. To the extent that users simply need to permit tightly integrated automated security tools to run, the need for extensive security awareness training may be reduced, or perhaps more accurately, refocused on

> ***Users not interfering with automated tools that are working to keep their systems secure.***

For example, users may perceive automatic updates as excessively time consuming or inconvenient and may defer installing them, thereby interfering with the vendor patching process. As another example, users may completely disable a vendor-installed firewall if they believe it may interfere with an application of interest. Others might change browser settings at the urging of particular web sites to enable useful (but risky) technologies blocked by default by the browser. Those 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 Two

Goal two, 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.

Where we diverge from the plan's findings, however, is at or about line 309, which ties cybersecurity 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 work place needs.

Computer Science is one STEM area that's an obvious exception. Cybersecurity practitioners certainly benefit from an understanding of computer science topics, but often the sort of computer science that's taught in second schools or higher education is abstract or theoretical, and doesn't deal with 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 those 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 that there may be insufficient emphasis on "soft skills," including collaboratively working with users, verbal and written communication skills, aligning cyber security efforts with business drivers, and effectively working with co-workers and management to plan and implement cybersecurity solution strategies.

Unfortunately, given the ever-increasing government emphasis on regulation and compliance (rather than technical cybersecurity), 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 that's a trend that we certainly hope doesn't continue or become even more pressing.

We'd 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 who lack hands-on practical experience are legion. Nothing substitutes for practical experience, but as we all know, unless you already *have* experience you often aren't qualified to get a position where you can *get* experience. We need to break that 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 chances for students to actually "get their hands dirty" and understand what industry is struggling with when it comes to cybersecurity.

Moving ahead to about line 409 and following, when it comes to graduate-level cybersecurity research and development, we would like to urge an emphasis on *data-driven* cybersecurity research. What distinguishes scientific scholarship from speculative philosophizing is hard data. In our experience, often simulations (based on overly-simplified models) replace true hard field data in the cybersecurity research field. Collection and analysis of actual hard data is far more likely to lead to insights, and solutions, than simulated data based on simplified abstract models. Cybersecurity inherently involves corner cases and unexpected artifacts and things that are *not* explicitly well modeled — you're only going to encounter data for those sort of events if you're observing and working on real datasets, and that's something that will normally require the sort of academic/industry collaboration we've previously urged.

IV. Comments On Goal Three

Goal three 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, "warehousing" them at non-sensitive make-work tasks until their clearance can be successfully completed. That's a process that 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 get 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 3.2, at or about line 575, that the draft plan recommends "Study[ing] the application of professionalization, certification, and licensing standards on cybersecurity career fields."

While becoming certified has substantial value in that it forces the applicant to systematically review the body of knowledge covered by the certification program, while also establishing norms of professional behavior for a field where the public may not be able to independently and transparently assess practitioner competence, 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 required 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 economically expensive to complete, thereby potentially acting as a screen that might disproportionately impact lower socio-economic-status groups/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'd also note that to the extent you impose daunting formal requirements for someone to become a cybersecurity professional, you limit the pool of potentially available employees. If you couple that constraint with a voracious federal appetite for credentialed cybersecurity professionals, you will not be helping industry 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 for you on that section:

— With respect to conferences, workshops, symposia, etc.: please understand that the cybersecurity community already has many, many, events of the sort you envision, to a degree where simply trying to identify an available data 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. Unfortunately, that sort of extreme travel schedule directly interferes with actual productive work on cybersecurity issues at home institutions, and tends to be expensive.

Please don't exacerbate this problem by creating new "must-attend" cybersecurity events. Please work to integrate the activities you envision with one or more of the *existing* cybersecurity events that are already broadly attended, and if anything, provide funding to allow those who may be interested and ready to contribute to participate even if internal funding isn't available to underwrite their attendance.

— 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 shared 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 and working together regardless of geographic location.

We need the help of our colleagues abroad, and they need in turn need us, but in many cases we may not even know each other (although MAAWG has attempted to set an example/"eat its own dog food" in this regard, routinely holding at least one of its three meetings each year in a European venue).

— We'd also like to flag the issue of how we're to keep cybersecurity professionals up-to-date with respect to ongoing operationally relevant cybersecurity information. By its very nature, many of the operationally relevant security considerations 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 his or her peers, those peers may effectively need to "rediscover fire" on their own, time after time, even when what they're (re)discovering is common knowledge among a more limited and trusted set of cybersecurity practitioners.

This problem is particularly acute for isolated cybersecurity practitioners who work for small firms that lack the budget or critical mass to help their cybersecurity practitioners become introduced to, and trusted by, more elite/vetted cybersecurity community activities.

If you want to truly improve the ongoing quality of operational cybersecurity staff expertise, work on tackling the issue of how *operationally relevant sensitive cybersecurity information* may be *scalably* 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 this sort of sharing, in that they require an affirmative action by users (logging in and browsing conversation threads) rather than having relevant cybersecurity intelligence automatically "pushed" to users the way 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 won't 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 get in touch.

Sincerely,

/signed/

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