CITIZENS CRIME COMMISSION
OF NEW YORK CITY

April 8, 2013

Dear Dr. Gallagher and Members of the Cybersecurity Framework Team:

Thank you for holding the framework workshop on April 3rd, 2013. It was very helpful for formulating comments in response to the RFI. Several speakers at the workshop noted the importance of including the widest possible audience for the Cybersecurity Framework conversation, so the following comments were prepared with this in mind, using minimal jargon and additional explanation of security management issues where necessary.

There are a daunting number of technical, managerial and behavioral issues to tackle in the cybersecurity space but a preponderance of evidence suggests that the greatest gap in cybersecurity is poor user behavior. This is a frustrating and even contentious issue for security personnel because to date, training programs such as security awareness programs have been met with limited results, leading some security personnel to even conclude that bypassing users altogether is the solution.

However, the Cybersecurity Framework Initiative presents a unique opportunity to address the critical issue of engaging users in more secure behavior, often referred to as cyber hygiene. Cyber hygiene was specifically referred to by several of the presenters throughout the workshop and has been identified as the number one problem to tackle by leading experts in the field of information security. Former NSA Director Mike McConnell noted that 80-85% of recent breaches are due to poor cyber hygiene among users and three members of the framework team that kicked off the workshop alluded to this issue as well:

- Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator noted that we are looking to 'raise the baseline of cybersecurity for all'
- Jane Lute, Deputy Secretary, Department of Homeland Security, noted that there would be 8 subgroups working on the framework including incentive programs 'for as wide of an audience as possible'
- Patrick Gallagher, Under Secretary of Commerce for Standards and Technology and Director of NIST, mentioned that there are three key initiatives for the framework – managing risk, cyber hygiene, and tools and techniques to support goals. Only the third of these is primarily a technical problem. The first one is primarily a management problem and

the second one is a daunting task that requires an overhaul of all user behavior.

Specific Recommendations for Tackling the Cyber Hygiene Problem

The following recommendations are based on a commonly held formula for security management:

Consequences = the point where Threat successfully exploits Vulnerability

Where:

Consequences range from temporary inconveniences such as down time on individual servers to catastrophic loss of intellectual property,

Threats include every problem-causing actor/action from hacker actions to malware payloads to natural disasters, and

Vulnerabilities are the points of weakness in our systems and processes, including software bugs, mobility of hardware, risky methods of connecting to the network, overly simple passwords, and poorly trained/careless user)

As Tony Sager, Director at the SANS Institute, noted during the workshop, we are living in the 'golden age of threat' – we have never known more about the attacks on our computers and related systems. It overwhelms us as every day there are new variants on old attacks that are just different enough to slip through a corporate crack. What's surprising, however, is that while there are new tweaks to old threat formulations emerging constantly, nearly all variants old and new are dependent on the same vulnerabilities being in place. Specifically hackers still rely on users having guessable passwords or a willingness to click on links in email messages or some other poor behavior that provides the opportunity to deliver a blow to the organization. This is true for all users from home computer users to users working in top governmental agencies. Accordingly, improving user behavior even slightly could reduce the overall attack surface for all parties involved.

However, as noted above, the results from traditional security awareness training programs are mixed, so clearly there is room for improvement to our current approach. Some issues to consider in developing more effecting training programs include the following:

- Many security awareness programs are driven by regulatory compliance rather than by the most pressing issues facing the organization which may lead to a lack of effectiveness overall.
- The majority of awareness programs are lecture based when hands-on activities are far more effective for experiential learning.
- Many security awareness programs give users credit for attendance rather than for active changes in behavior.

Companies that have had success with training programs have further found that:

- Teaching individuals how to protect information of personal interest will have a greater impact on their behavior at work than training focused exclusively on protection of work-related data
- We learn through repetition so programs that require frequent training are more successful than organizations that offer training upon employment or less than once a year
- Providing rewards for good behavior works. Requiring remedial training for poor behavior also works.
- Including internal tests, for example sending out fake phishing attacks to see how employees respond is also effective.

Given that the behavioral problems tend to be fairly common across all organizations, a robust training program built on best practices could be developed for all members of the sixteen critical infrastructure sectors and rolled out to all voluntary participants.

As an additional step, there could be a centralized social marketing campaign (e.g., to paraphrase Smokey the Bear, "only you can prevent cybercrime") to engage users in being a part of the solution to the larger cybercrime problem. This could be offered to all users across the country as all computers are connected to all other computers on the Internet. Again, the emphasis of such a program should be action-oriented – not lecture based. And it should be comprehensible by the majority of all computer owners. Another point relevant to such a program is that results from my own research indicate that simply raising a user's awareness of a problem can build fear and actually reduce the likelihood that the individual will act responsibly. Fear alone makes people want to avoid a situation altogether. However, the likelihood that a user will take action is vastly improved when awareness of the problem, awareness of how the user's actions impact others plus the specific knowledge necessary to change behavioral patterns are all provided at the same time. When users truly understand how interconnected everything is and how one small change in their own behavior, like password protecting a mobile device, can have a significant

impact on their employer as well as their personal security, they are far more likely to comply. Also, when users understand that there is an initial learning curve but after that security management can become as routine as fastening a car seatbelt or locking the doors and windows on a house, they are more likely to comply.

Taking the time to educate users about the role that they can play could make a real impact. In addition to launching a behavioral change program (as opposed to a security awareness program), the framework could also include incentives to other parties that can play a part in reduction of vulnerabilities. For example, there could be a request for voluntary compliance with security standards among software developers with the reward of being included on of preferred vendors. Similar incentives could be offered to cloud storage companies who engage in security best practices such as monitoring for suspicious activity.

Finally, another reason why a change in behavior is critical as we move forward is the fact that lines between device ownership and device use are blurring by the growing trend toward use of personal devices for work. In a recent Cisco survey of 1000 working Americans with smartphones, it was revealed that 39% don't password-protect their phones and 52% access unsecured wi-fi networks with their devices, and 92% of those surveyed use their smartphones for work purposes at least occasionally while 62% use their smartphones every single day for work. Again, it is impossible to expect the small population of already over-taxed security experts to save all users from themselves. It is important to incentivize and inspire individuals to start taking responsibility for the very powerful devices they carry around with them all the time.

Thank you again for the opportunity to participate in the framework development process. I would be most happy to participate in additional ways that might be helpful.

Good luck with the process as you move forward on this most important initiative.

Best Regards,

Amy Williams, PhD
Director of Cyber Crime Initiatives
Citizens Crime Commission of NY