Some Suggestions for a Cybersecurity Framework to Improve Critical Infrastructure Cybersecurity

James A. Lewis, March 2013

The President's Executive Order of February 2013 is a major development and offers a real opportunity to improve U.S. national security – if it is implemented correctly. There are only three metrics for judging success: is the number of network penetration by attackers decreased ("did they get in'), were they able to disrupt service or data once they are in, and did the amount of information they were able to exfiltrated decrease. These quantitative metrics focus on outcomes. Measure that cannot be shown quantitatively to affect these outcomes should not be in the cybersecurity Framework called for by the EO. Here are six ideas on how to shape an effective Framework.

1. The Framework should be short, not encyclopedic. Keep the Framework to less than ten pages. Existing guidance cybersecurity is often too long to be workable. The target audience for the Framework is the C-Suite, not a technical or engineering audience, and it should be drafted appropriately.

2. A Framework is not a survey or an election, and "lead by following" is a non-sequitur. The elements of the executive branch charged with cybersecurity must begin work on a Framework with a vision of what is necessary and then adjust or expand this based on comments received.

3. The Framework should focus on computer network security, not critical infrastructure performance. The Framework should not duplicate the National Infrastructure Protection Plan (NIPP). It should concentrate on ensuring that networks cannot be penetrated and misused, not on quality or reliability of infrastructure services – no requirements for ensuring minimal downtime for servers, for example.

4. The Framework should not be drafted as a precursor to regulating the entire dot.com space. These should be written as voluntary measures and any mandatory application of the Framework should be limited to a small number of facilities. The requirements of Section 10 of the Executive order should not apply to all eighteen of the critical infrastructure sectors. One model for such limitation would be to require the mandatory application of the Framework to four or five sectors: electrical power, telecommunications, finance, government services, and perhaps some transportation networks. Any mandatory application could be further limited to defined geographic areas of critical importance for national defense.

5. A Framework should tell companies that they must take the following steps to be secure:

- "Whitelist" applications that are permitted to run on company networks. Whitelisting is already a feature of anti-virus products that many companies have simply not used. Fears that Whitelisting will disrupt operations are exaggerated.

- Automate and track the updating and patching of operating systems and applications. Failure to uniformly update is widespread, and uneven updating leaves open crucial vulnerabilities.

- Restrict "administrator privileges" on networks, including the ability for administrators to have remote access to management and control functions.

- Inventory of devices on the network, including wireless devices, and their configuration and security status. "Forgotten" or infrequently used devices are likely to miss updates and be a source of vulnerability. Wireless devices are inherently at greater risk.

- Use enhanced multifactor authentication using either device-based authentication or one-time passcodes. There will be objections that requiring adequate authentication will slow down or complicate operations; the same is true of putting locks on trucks and doors. It is time to grow up regarding the use of passwords. We can no longer rely on them.

- Adopt continuous monitoring of system activity and security status to allow for rapid mitigation of vulnerabilities.

- Develop arrangements with internet service providers for screening and defense for traffic coming from the public network. Close scrutiny of the contractual arrangements to ensure an appropriate level of security services are especially important for cloud services.

- Create mechanisms to obtain information to identify potential attacks.

- Develop plans and techniques (perhaps with service providers) for dealing with DDOS events.

- Build an autonomous data recovery capability for high value data not connected to the network and not automatically updated (automatic updating can result in an "infection" being copied to the supposedly 'sterile" backup data).

6. These requirements are applicable to all networks and there is good data to show that their application will make networks more secure. Other measures in addition to these may be identified in other submissions, but NIST should review these suggestions by asking if they can be demonstrably shown using quantitative data to reduce penetration, disruption and exfiltration (the three core metrics for security). The framework should not be a collection of "nice-to-have," measures, but focus on the five or six key mitigation strategies that already work. The development of sector specific measures should be left to the second phase of the EO process, when the general Framework is given to sector-specific agencies to develop, in partnership with companies in their sector, specific measures applicable to that sector and that take the business need and requirements of companies in that sector into account.