ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

To the White House Cyber Security Review Team:

Recommendations

The Electronic Frontier Foundation has three main recommendations to the White House Cyber Security Review Team.

Recommendation 1: *Ensure that Government security programs are open, transparent and accountable, and that they protect citizen privacy and civil liberties*

The United States Government should ensure that its civilian cybersecurity policies place an extremely high priority on transparency, accountability and protection of individuals' privacy and civil liberties.

1. Ensure that the Federal Government's cybersecurity programs are founded upon and guided by analytical risk assessments.
2. Publish these risk assessments (brief embargo periods may be appropriate if drastic, unexpected and unmitigated risks are discovered).
3. Ensure that citizens' privacy and civil liberties are explicitly considered amongst the assets to be defended in risk assessments.
4. Publish the steps that departments and infrastructure operators are required or encouraged to take to improve security. Provide clear explanations of the rationales behind these steps.
5. Publish the full results of security audits and investigations (after a brief embargo period during which security vulnerabilities would be fixed)
6. Beware of large, monolithic "cybersecurity" projects.
7. If the Government funds the creation of new cybersecurity systems, they should be published under free/open source licenses.
8. Exercise caution in deciding the appropriate scope of the National Security Agency's role, which has a highly secretive culture that does not necessarily mesh well with the best practices in private sector civilian security or meet the transparency obligations of good governance.

Recommendation 2: *Ensure that any consideration of liability for security vulnerabilities or other incentive mechanisms for private software vendors not discourage the production of free/open source software.*

Recommendation 3: *Consider setting up a government "Open Source Security Institute", that identifies open source codebases that are critical to the nation's cybersecurity, and works to enhance the security of those codebases.*

454 Shotwell Street • San Francisco, CA 94110 USA
+1 415 436 9333 +1 415 436 9993 www.eff.org information@eff.org

Our Reasoning

The task of improving security will require sustained and detailed commitment across many entities and over many years. This task cannot be done well – and with proper attention to the government's duty to secure privacy and civil liberties while it secures the information infrastructure – if it is driven by events and a crisis mentality. The rhetoric of crisis and urgency can lead to intemperate, overreaching actions.

Thus, we emphasize institutional processes over any specific technical actions. And these institutional processes must be transparent and accountable, for many reasons. First and foremost, transparency and accountability are essential to a democracy. Second, good policy here requires broad participation in deciding what to do, because improving network security is not merely a technical issue. It will require the concerted effort of many people, which in turn will require their meaningful input over time. Moreover, the ascendant role of the National Security Agency in current cybersecurity efforts means that substantive values like privacy and civil liberties will be at risk throughout the entire process. Only a transparent, accountable process can allow any sort of counterweight to the drumbeat of "cyberwarfare" and "cybercrime."

Finally, it is already clear that secrecy and overclassification of information have severely hindered past network security efforts, as evidenced by widespread concern about the secrecy surrounding the Comprehensive National Cybersecurity Initiative (CNCI). *See, e.g.*, Victoria Samson, Senior Analyst, Center for Defense Information, *The Murky Waters of the White House's Cybersecurity Plan: "The Comprehensive National Cybersecurity Initiative: What You Don't Know May Hurt You,"* http://www.cdi.org/program/document.cfm?documentid=4345&programID=68&from_page=../friendlyversion/printversion.cfm (July 23, 2008).

We should candidly recognize the tension in this area and consciously bias the design toward openness, toward democracy, toward privacy and civil liberties, because recent history teaches us that the combination of intelligence and law enforcement pressure is far more powerful in difficult times than the voices of liberty and freedom.

This bias should inform remediation priorities. Decisions about basic security hygiene — the digital equivalent of locking doors or putting valuable assets in safes — are relatively unlikely to violate privacy or other civil liberties standpoint and thus can be made fairly quickly. Indeed, many such decisions have already been made, but not implemented. As the Government Accountability Office reported last year,

"[F]ederal agencies continue to confront long-standing information security control deficiencies. Most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. In addition, agencies did not always effectively manage the configuration of network devices to prevent unauthorized access and ensure system integrity, install patches on key servers and workstations in a timely manner, assign duties to different individuals or groups so that one individual did not control all aspects of a process or transaction, and maintain complete continuity of

operations plans for key information systems. An underlying cause for these weaknesses is that agencies have not fully or effectively implemented agency-wide information security programs. As a result, federal systems and information are at increased risk of unauthorized access to and disclosure, modification, or destruction of sensitive information, as well as inadvertent or deliberate disruption of system operations and services. Such risks are illustrated, in part, by the increasing number of security incidents experienced by federal agencies. . . . Federal agencies could implement the hundreds of recommendations made by GAO and IGs to resolve prior significant control deficiencies and information security program shortfalls." Government Accountability Office, Testimony Before Committee on Oversight and Government Reform, House of Representatives, *Information Security: Although Progress Reported, Federal Agencies Need to Resolve Significant Deficiencies,* GAO-08-496T, at 3 (Feb. 14, 2008). http://informationpolicy.oversight.house.gov/documents/20080214131840.pdf
Similarly, decisions about addressing long-term vulnerabilities through increased funding for fundamental research are far less likely to threaten privacy and civil liberties, and again can be made in a shorter time frame.

In contrast, decisions about very large scale intrusion detection systems and other cybersecurity techniques that involve surveillance of private traffic inherently raise serious privacy and civil liberties issues and thus require much more analysis and public discussion. Proposals to expand online identity verification or authentication would similarly trench upon well-recognized constitutional rights to speak and associate anonymously. In some foreign countries, anonymity may be one of the few practical protections for political and religious dissidents; the United States should not promote policies that are likely to chill speech abroad and at home.

The Importance of a Transparent and Accountable Government Security Culture

One of the oldest questions in computer security is whether security is better served by keeping secret as many aspects as possible of one's software and operations, in the hope that that secrecy will confound adversaries – or by keeping as few secrets as possible, on the theory that every secret is hard to keep and defenses must be robust even against a well-informed adversary. Recent research on the subject has suggested that security can in principle be reached by either route, and that other issues of organizational and technical context may determine which road to security is shorter.[1]

We believe that civilian governmental cybersecurity programs must aim to achieve security by the route of openness, and the use of transparent and accountable processes. The reasons include the special duties that governments have to their citizens, such as the duty to guard privacy and civil liberties, and the duty to be accountable in the use of taxpayer's dollars. They also include the fact that government programs are by their

1 Ross Anderson (2002) "Security in Open versus Closed Systems – the Dance of Boltzman, Coase and Moore", Proceedings of Open Source Software: Economics, Law and Policy, at http://idei.fr/activity.php?r=1898

nature not competing in a marketplace, where strong financial incentives may be present for the clever use of secretive practices. Moreover, the sprawling nature of the nation's infrastructure greatly decreases the likelihood of keeping secrets against adversaries, and greatly increases the potential benefits of constructive scrutiny from all corners.

There are many ways that these objectives could be reflected in the design of the Federal Government's cybersecurity programs, but here are some important measures that we believe should be implemented:

Ensure that the Federal Government's cybersecurity programs are founded upon and guided by analytical risk assessments

Computer-related security vulnerabilities derive from diverse causes. They include subtle bugs in computer programs, which allow those programs to be crashed or subverted for purposes other than those they were intended for; software design flaws (which are harder to fix than mere bugs) that have the same consequences; institutional processes that rely on software systems without sufficient awareness of potential security issues with that software; and the fact that most human beings do not naturally engage in the type of semi-paranoid, skeptical technical thought that is necessary to understand security properly.

The difficulty of addressing these causes ranges from very difficult up to impossible. In real-world settings of any scale, security will always be imperfect. The most sensible way to decide what level of resources to allocate to security problems, and which problems to address, is to perform risk assessments that identify the nature of threats, their probability and severity, and then to set about mitigating the most serious threats. These risk assessments must be regularly updated and subjected to scrutiny and review to ensure that they are as accurate as possible.

The Federal Government should publish its risk assessments

By publishing its own cybersecurity risk assessments, the Federal Government can achieve several things:

- Allow peer-review from independent computer security experts working in industry and academia
- Encourage input from these parties, who may have unique insight or expertise on how best to mitigate identified threats
- Demonstrate to taxpayers that their money is being directed towards the most critical security threats, and not toward “security theater”

When risk assessments identify threats that are surprising to security experts, serious and unmitigated, it may be appropriate to briefly embargo those results, giving time for hasty mitigation. Medium to long-term embargoes are unwise.

Ensure that citizens' privacy and civil liberties are explicitly considered amongst the assets to be defended in risk assessments

Government departments often handle large amounts of information about members of the public. Privacy concerns are already addressed within the practices of many organizations and departments, but these issues may benefit from being included as a part of systematic analytical risk assessments.

Identity theft is one of the major objectives of those who deploy malicious code on the Internet at present, and mitigation of that risk should be considered a cybersecurity objective even where private sector computers are the major target.

Including privacy and civil liberties assets in risk assessments may occasionally improve decisions about mitigation strategies, such as correctly illuminating the trade-offs of proposals for widespread surveillance, data retention or other security measures that have impacts on civil liberties.

Publish the steps that departments and infrastructure operators are required or encouraged to take to improve security. Provide clear explanations of the rationales behind these steps.

Details of the cybersecurity risk mitigation strategies that are deployed within government departments or private infrastructure operations should be published for the same reasons that risk assessments should be published (peer review, encouragement of constructive input, taxpayer accountability).

Furthermore, systematic documentation of how security efforts are playing out in other departments and organizations may offer valuable lessons for other parts of the nation's cyber defense effort.

Publish the full results of security audits and investigations

The results of security audits will contain numerous examples of bugs found in software; organizations running old, unpatched versions of software; management and employees not understanding the security aspects of their roles; and other results which may seem "embarrassing" to the departments in question.

These results are normal, and they should be published in order to demonstrate that cybersecurity programs are achieving results, and to allow longer term independent measurements of security improvements and the cost effectiveness of cybersecurity programs.

Beware of large, monolithic cybersecurity program expenditures

Traditional security contractors will inevitably encourage the Federal Government to spend large amounts of money on specific cybersecurity programs, perhaps including

specialized firewalls, intrusion detection systems, host auditing and anti-virus mechanisms. There are several reasons to be cautious about these kinds of projects.

First, the more complex a system is, the less likely it is to be secure and the greater the cost required to test, debug, and audit it. In computer security terms, bigger is not better.

Second, if a cybersecurity system (software, hardware, or both) is useful to the Federal Government, it should be useful to numerous other organizations. It follows that most or all of the Federal Government's cybersecurity needs should be realizable without producing new expensive systems. It also follows that if the Federal Government *is* commissioning new systems, the private and independent computer security sector should be interested in using them too.

<u>If the Government funds the creation of new cybersecurity systems, they should be published under free/open source licenses.</u>

Following from the last point above: if the Federal Government is funding the production of novel cybersecurity systems, the expectation should be that these systems will be useful to the community more generally; a lack of such interest should be regarded as a yellow flag against the project.

In order to appropriately test the security community's interest in any code the government is commissioning, to ensure the quality of that code, and to maximize the taxpayer's value for that expense, any such software should be published under an open source license.

<u>Organizational architecture: the role of the National Security Agency (NSA)</u>

EFF is concerned that the intelligence community – especially the NSA – will continue to dominate the cybersecurity effort. As former Director of the National Cybersecurity Center Rod Beckstrom recently stated,

"NSA effectively controls DHS cyber efforts through detailees, technology insertions, and the proposed move of the NPPD and the NCSC to a Fort Meade NSA facility. NSA currently dominates most national cybersecurity efforts. While acknowledging the critical importance of NSA to our intelligence efforts, I believe this is a bad strategy on multiple grounds. The intelligence culture is very different than a network operations or security culture. In addition, the threats to our democratic processes are significant if all top level government network security and monitoring are handled by any one organization (either directly or indirectly). During my term as Director we have been unwilling to subjugate the NCSC underneath the NSA. Instead, we advocated a model where there is a credible civilian government cybersecurity capability which interfaces with, but is not controlled by, the NSA."

EFF understands Mr. Beckstrom as saying that the intelligence culture is hostile to transparency and accountability, and that undue organizational concentration is

dangerous to democracy. We agree.

The NSA's approach to security has very much favored the path of secrecy over the path of openness, which should be a foundation of the Government's plan for civilian cybersecurity. The NSA lacks any credibility in the defense of civil liberties and privacy, or for a role that requires security defense to be conducted openly.

A critical part of the NSA's mission is to intercept communications or otherwise gather intelligence from computer systems and telecommunications networks. Security vulnerabilities aid the NSA's surveillance mission, especially abroad. Although we cannot know for sure because of the secrecy surrounding its methods and operations, it is reasonable to assume that the NSA has historically concealed its knowledge of vulnerabilities in order to better carry out surveillance. Indeed, some security experts have argued that the NSA's warrantless wiretapping program may have created additional security vulnerabilities in our domestic networks.[2] Under current law – as well as the Bush Administration's extravagant claims of "state secrets" in litigation aimed at redressing statutory and constitutional violations – the NSA's activities are hidden from meaningful public oversight. It makes no sense to entrust our nation's IT infrastructure to a virtually unaccountable agency with a track record of violating civil liberties.

Some argue that the NSA should dominate cybersecurity remediation because it has unique technical competence. EFF does not believe that this has been demonstrated. The historical record shows that the NSA once had unique technical competence in areas such as signals intelligence, cryptography, and cryptanalysis. There is less evidence to suggest that it has possessed unique levels of competence in software and network security, or that it has been able to retain the best talent in an era when security-related skill sets have come into high demand in the private sector.

In addition, it seems clear that lack of technology is not responsible for the poor progress in federal computer security remediation. Most government networks use commercially available software. Yet a GAO report found that federal agencies are not using commercially available technologies to protect sensitive information. Although OMB and NIST had set policies and published guidelines for encrypting data,

"none of the agencies had documented comprehensive plans to guide encryption implementation activities, such as inventorying information to determine encryption needs; documenting how the agency plans to select, install, configure, and monitor encryption technologies; developing and documenting encryption policies and procedures; and training personnel in the use of installed encryption. Further, our tests at 6 selected agencies revealed weaknesses in the encryption implementation practices involving the installation and configuration of FIPS-validated cryptographic modules, encryption products, monitoring the effectiveness of installed encryption technologies, the development and documentation of policies and procedures for managing these

---

[2] S. Bellovin, M. Blaze, W. Diffie, S. Landau, P. Neumann, and J. Rexford (2008), "Risking Communications Security: Potential Hazards of the 'Protect America Act,'" *IEEE Security and Privacy*, 6(1) 24-33, at http://research.sun.com/people/slandau/PAA.pdf

technologies, and training of personnel in the proper use of installed encryption products. As a result of these weaknesses, federal information may remain at increased risk of unauthorized disclosure, loss, and modification." Information Security: Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains, at 4-5, GAO-08-525 (June 2008)
http://www.gao.gov/new.items/d08525.pdf

In short, agencies are not doing basic security hygiene or "target hardening"; known problems with known solutions are not being addressed. This is more accurately framed as a failure of coordination, management or implementation, than as a failure of technical competence.

Software Vendor Liability for Security Vulnerabilities

One category of proposals for government action to improve cybersecurity within the private sector revolves around the idea of introducing a regime in which software producers take on liability for vulnerabilities in the code they sell.

The economic theory underlying these liability proposals is that computer software may exhibit market failures of the Akerlofian "market for lemons" type,[3] wherein purchasers of software cannot know the true quality and extent of the vendor's security engineering practices, and therefore cannot correctly value a more secure software product over less secure software.

Liability regimes or other related incentive schemes may or may not be an effective way for the Federal Governments to improve the practices of the private software industry. We have one concern, however, about these proposals.

Free and open source software has become a widespread phenomenon in the computer industry. It involves parties (including hobbyists, university researchers, for profit firms and even government departments) who collaborate to produce software and publish it under copyright licenses that allow others to use, modify and redistribute the code.

In economic terms, free and open source software is an example of the private, voluntary production of public goods. Individuals and organizations are motivated to participate for diverse reasons, but in general their activities produce very significant positive externalities for the rest of society. The creation of a security liability regime (even a liability regime with an exception for "not for profit" software production) could chill the participation of for-profit firms in this activity that produces very significant social spill-over benefits.

---

3 See George Akerlof (1970), "The Market for Lemons: Quality Uncertainty and the Market Mechanism", *Quarterly Journal of Economics,* 84(3) 488-500.

We therefore urge that your analysis of software liability regimes recognize the special situation of software published under free/open source copyright licenses and consider the value of a liability exemption.

Consider creating an "Open Source Security Institute"

Open source software forms a large part of the nation's computer infrastructure. Somewhere over 50% of the nation's servers function at least in part on open source code.[4]

As discussed above, the production of free/open source software is an example of the private, voluntary production of public goods. Because open source software authors cannot internalize the full value of the software they produce, they will in general have fewer financial resources for those projects and suboptimal incentives to work on those projects.

Abstractly, these economic circumstances would suggest that governments should take active steps to support and encourage the production of free and open source code, although in practice there are serious informational barriers to governments doing this directly ("Should a government fund the production of an free, open source word processor? Perhaps that would pass a cost/benefit test very clearly, but which of the existing competing projects should be funded?").

It is likely that by funding security engineering work for existing successful free/open source projects the Government would be able to greatly enhance the security of 50% of the nation's servers, producing benefits that were disproportionately greater than the number of dollars spent, without having to pick winners from prospective projects.

We therefore believe the White House should investigate the possibility of setting up an Open Source Security Institute along the following lines:

1. Identify which free/open source software codebases are currently in the most widespread use in the United States
2. Perform cybersecurity risk assessments on the use of that software, to determine which open source codebases are currently most critical to the nation's cybersecurity
3. Perform security audits and engineering work on those projects, either by contract or by performing the work directly

---

4 Apache, an open source web server, currently powers 48.5% of the world's web servers (http://news.netcraft.com/archives/2009/03/15/march_2009_web_server_survey.html). Linux, OS X and other UNIX operating systems make up 50% of server sales expenditures (http://www.theregister.co.uk/2009/02/25/idc_q4_server_numbers/print.html), and these operating systems are comprised, in part or entirely, of open source software.

Respectfully submitted,

Lee Tien
Senior staff attorney
tien@eff.org

Peter Eckersley
Staff technologist
pde@eff.org

Electronic Frontier Foundation