EINSTEIN INTRUSION DETECTION SYSTEM: QUESTIONS THAT SHOULD BE ADDRESSED

July 2009

This paper calls on the government to release information about the Einstein intrusion detection system for government computers. It poses questions about the role of the National Security Agency in the Einstein program, the scope of the latest version of the Einstein system, the legal authority for the system, and the impact of Einstein on the privacy of people who communicate with the government. It also calls for the release of any legal opinions and certifications about the lawfulness of Einstein intrusion detection activities, and for release of the privacy guidelines governing the system and of privacy training materials given the people who may come into contact with information derived from Einstein.

Recent press reports in the *Washington Post*[1] and *Wall Street Journal*[2] indicate that the federal government is putting in place a new intrusion detection system to help secure civilian networks in the .gov space. This system, dubbed "Einstein 3," is the successor to an existing system – "Einstein 2" -- now deployed by the Department of Homeland Security and soon to be deployed by other federal agencies. While Einstein 2 poses privacy concerns that have not yet been fully resolved, Einstein 3 both heightens those concerns and poses additional questions of its own.

According to a May 19, 2008 Privacy Impact Assessment,[3] Einstein 2 detects malicious computer code in network traffic using pre-defined signatures of such

[1] http://www.washingtonpost.com/wp-dyn/content/article/2009/07/02/AR2009070202771_pf.html.

[2] http://online.wsj.com/article/SB124657680388089139.html#printMode.

[3] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf.

code and alerts the U.S. Computer Emergency Readiness Team ("US CERT"). Some of those signatures include personally identifiable information ("PII") and some of the alerts from Einstein 2 to US CERT also include PII. Previously unknown attack signatures cannot be detected by Einstein 2, and, as a result, anything new gets through the system until the database of attack signatures is updated to include it. According to the PIA, Einstein 2 will be deployed at participating federal agency Internet Access Points.[4]

Like Einstein 2, Einstein 3 will rely on pre-defined signatures of malicious code that may contain PII. However, Einstein 3, unlike its predecessor, will have the added capability of reading the content of email and other Internet traffic, according to the *Wall Street Journal* story. This raises serious privacy concerns. In addition, while its predecessor merely detected and reported malicious code, Einstein 3 is to have the capability of intercepting threatening Internet traffic before it reaches a government system, raising additional concerns. This capability is reportedly based on a National Security Agency program. According to press accounts, Einstein 3 will operate inside the networks of the telecoms, but it is not clear whether this is the same as Einstein 2 or not.

According to the press accounts, AT&T would be contracted by the government to test portions of Einstein 3 and is seeking assurance from the Department of Justice that this activity does not violate the law.

Some policymakers are reportedly studying potential changes to current surveillance law to permit the scanning of private Internet traffic, for security purposes only, without an individualized court order. The Senate version of the Intelligence Authorization Act for FY 2010, S. 1494, reported on July 22, does not propose any such changes. Instead, it calls for reports to Congress about the privacy impact of Einstein and any other similar cybersecurity programs as well as information about the legal authorities for the programs and about any audits that have been conducted or are planned for the programs.

[4] It is unclear to CDT whether this means that Einstein 2 operates on privately owned and operated equipment or on government equipment. More importantly, it is unclear whether the point at which Einstein is deployed handles only government traffic or could carry both government and private-to-private traffic.

The recent press accounts about Einstein raise a number of questions that should be answered publicly:

Role of the NSA and Private Sector

- What is the role of the National Security Agency in Einstein 2 and what role is contemplated for NSA in Einstein 3?
    - Who designed Einstein 2 and 3?
    - What information about individual communications does/will NSA receive or have access to under Einstein 2 or 3?
    - What limits will be put on NSA uses of such information?
- What is the role of the private sector in implementing Einstein 2 and 3?
- Do private sector companies that provide Internet access to the government have the capability to run Einstein or a similar security program? If not, are there any plans for helping them to develop that capability?
    - Can NSA supply the necessary attack signatures to private sector entities providing Internet access to the government?
    - What roles, if any, can be performed only by NSA?
- What private sector information other than attack signatures will be used in the Einstein 2 and the Einstein 3 programs?
- What safeguards will be put in place to ensure that the carriers that will be examining Internet traffic bound for government networks will not misuse that role?
    - What information will private sector network operators keep about the communications that appear to match attack signatures?
    - What safeguards will be put in place to ensure that network operators will not retain such traffic?
    - Will the contracts between the government and the carriers prohibit the carriers from retaining such traffic?
    - What would prohibit network operators from using Einstein for other purposes?

Minimizing Collection of PII

- Is it possible to ensure that only government traffic will be reviewed by Einstein

for intrusion detection and response? If not, what are the estimates of how much non-government traffic is likely to be reviewed?

- What audit mechanism will be put in place to assess the performance of Einstein 2 and Einstein 3?
- The Einstein 2 PIA indicates that some information that is undeniably PII – such as email address – will sometimes be collected, for example, when malicious code is in an email or an email attachment. The PIA also indicates that origination IP address and time stamp – which are widely regarded as personally identifiable information, but which the PIA characterizes as information in which a person has "no expectation of privacy" – will be routinely collected as part of communications that appear to match attack signatures. The Einstein 2 PIA also indicates that reports of security incidents that US CERT will disseminate to law enforcement and intelligence officials will include personally identifiable information related to the security incident but minimize other personally identifiable information collected with it. *See*, e.g., pp. 13 and 15-16 of the Einstein 2 PIA. Based on experience so far with Einstein 2, what personally identifiable information has been collected by US CERT, what has been disclosed to law enforcement and intelligence agencies, and what follow-up activities at those agencies have resulted?
- To what extent are Einstein 2 incident reports being used to open criminal investigations, and how often have those investigations resulted in successful prosecutions?
- What personally identifiable information – including IP addresses and time stamps – will be collected in connection with the Einstein 3? What rules will govern PII collection, retention, dissemination and destruction in Einstein 3?

Privacy Guidelines and Training Materials

- The Einstein 2 PIA indicates that US CERT reviews all attack signatures "in accordance with legal and privacy guidelines" before those attack signatures are employed to identify malicious Internet traffic. *See* p. 4. Will those guidelines be made public? If they are classified, will unclassified summaries that include references to the particular statutory sections that govern the program be made public?
- The Einstein 2 PIA indicates that US CERT analysts and others who might come

into contact with Einstein 2 information receive annual training on privacy, legal and policy issues specifically related to Einstein 2. *See* p. 21. Will this training material be made public? If it is classified, will an unclassified summary that includes references to the particular statutory sections relevant to this training be made public?

Legal Authorities

- Will Einstein 3 involve the scanning, scrutiny or examination of the content of communications? If so, what legal authority is relied upon for such activity?
- Is the Administration considering asking Congress for additional legal authority to facilitate Einstein 3?
- Has the Attorney General issued any certifications under Section 2511(2)(a)(ii)(B) of Title 18 that relate to Einstein? (Such certification would indicate to carriers providing assistance with Einstein 2 activities that no warrant or court order is required for such activities.)
- Has the DOJ Office of Legal Counsel issued any memoranda evaluating the lawfulness of Einstein activities, and will any such memoranda be made public, as was done with key OLC legal opinions governing detainee treatment?
- What is the relationship of FISA to Einstein 3? FISA comes into play when communications are accessed when a significant purpose of the surveillance is to collect foreign intelligence information. Is foreign intelligence collection a purpose of Einstein 3, and, if not, what relevance does FISA have to Einstein 3?

Notifying Those Who Communicate with the Government about Einstein

- How will notice of the collection of personally identifiable information in Einstein 2 and Einstein 3 be handled across agencies, and what steps will be taken to ensure that notice is meaningful and timely?
- What language will be used to notify users that their email to/from government employees may be monitored for security reasons, and may be saved or shared for the same reasons, and likewise for logs of their visits to government websites?
- What are the rules for agency use of the logs that may be developed in

connection with Einstein intrusion detection systems? (We understand that such logs would include IP address, date, and the page the user went to and came from. Is that correct?)

- What steps, if any, will be taken to protect the privacy of logs of visits to particularly sensitive government websites, such as those that provide information on HIV / AIDS or birth control?

Limits on Retention and Sharing of Information, and Auditing Einstein

- In what circumstances will PII derived from the program be shared for analytic purposes related to network security? In what circumstances will it be shared with law enforcement or with intelligence agencies?
- DHS is holding onto Einstein-generated data for three years, according to the Einstein 2 PIA. *See* p. 13. Apparent attempts at intrusion, however, happen all of the time – thousands of times per week. Given that frequency, could a more limited period of data retention be put in place, such as one covering a few months instead of a few years?
- What independent auditing procedures will be put in place to ensure that actions taken as part of the Einstein programs are justified, are limited to those machines that are a threat to government servers, and ensure that only the minimum amount of PII is collected and shared, and that is it done in accordance with the applicable PIA?

Conclusion

As both CDT and others have concluded, secrecy undermines the effectiveness of cybersecurity efforts, especially where the government is dependent upon private sector cooperation and partnership. In order to speed the implementation of effective cybersecurity measures, the Obama Administration should take the initiative in addressing these questions. It can do so through the early completion and release of a Privacy Impact Assessment covering Einstein 3, and through the release of other information and documents, including legal opinions assessing the Einstein programs. Congressional oversight should encourage Administration disclosure. So should private sector service

providers, who should be able to assure their non-governmental customers that security efforts designed to protect governmental networks will not infringe on the privacy or security of commercial and personal communications not directed to the government.

FOR MORE INFORMATION

Please contact: Gregory T. Nojeim, Senior Counsel, (202) 637-9800 x 113, gnojeim@cdt.org