Cybersecurity: An Examination of the Communications Supply Chain
Statement of Stewart A. Baker
Partner, Steptoe & Johnson LLP
Former Assistant Secretary for Policy, Department of Homeland Security
Former General Counsel, National Security Agency

Before the Committee on Energy and Commerce
Subcommittee on Communications and Technology
U.S. House of Representatives

May 21, 2013

Chairman Walden and Ranking Member Eshoo, I appreciate the opportunity to provide this statement today.

Protecting the information and communications (ICT) supply chain is not a new problem. It was a concern in the 1990s when I was General Counsel at the NSA; it had become far harder when I was Assistant Secretary for Policy at the Department of Homeland Security in 2005-2009. But it has never been more important or more difficult than it is today.

1. The Threat

I hope that there is no need to dwell on the unprecedented wave of cyberattacks that the United States has suffered in recent years. Intrusions on our networks have reached new heights. They have moved from penetration of government and military systems to wholesale compromises of companies, trade associations, think tanks, and law firms. Most of these attacks have been carried out for espionage purposes – stealing commercial, diplomatic, and military secrets on a massive scale.

This espionage campaign has paid dividends for our adversaries, and it's likely to pay more, because any network that can be compromised for the purpose of espionage can be compromised for the purpose of sabotage. The next time we face the prospect of a serious military conflict, we can expect our adversaries to threaten the destruction of computer networks – and the civilian infrastructure they support – inside the United States, probably before we have fired a shot. From the American point of view, this is a new and profoundly destabilizing vulnerability. From our adversaries' point of view, it is an exciting new weapon with enormous potential to neutralize many of our traditional military advantages.

To make things worse, one of the countries that the Obama administration has criticized most often for cyberattacks, China, is also a major supplier of increasingly sophisticated electronic equipment to the United States. Given the value of cyberespionage for waging both war and peace, it's only reasonable to assume that every potential adversary asks itself whether it can make the job of its cyberwarriors easier by tinkering with electronic gear before it's shipped to the United States. Or, as I put it in *Skating on Stilts*, a book about technology challenges to

policymakers, if the "countries that [view] us as an intelligence target … could get their companies to compromise U.S. networks, they'd do it in a heartbeat."

That, at least, has not changed. And it is the most troubling supply chain problem we face.

But there's another that is also of concern. As electronics producers diversify their suppliers to the global lowest bidder, the risk grows that some of those suppliers will be irresponsible, cutting corners on quality or actively substituting inferior parts to boost profits. If our military electronics fail in a crisis, it matters little whether the failure was caused by deliberate sabotage or a bad outsourcing decision.

Either way, the security of our electronics supply chain is critical.

2. Partial Regulatory Authority -- CFIUS and Team Telecom

For policymakers, threats to the supply chain have most often arisen when foreign companies purchase U.S. suppliers. That's because U.S. law requires a national security review of such acquisitions by the Committee on Foreign Investment in the United States, or CFIUS. When I ran CFIUS, we aggressively used our authority to negotiate "mitigation" agreements with foreign purchasers to reduce the supply chain risk, something I discussed in *Skating on Stilts*:

> [A]llowing foreign companies to take up critical positions in U.S. computer and telecommunications networks, either as suppliers or as service providers, raised serious national security issues. At the same time, globalization was relentless. The old days, when AT&T provided local and long distance service—and made all the equipment on the network—were long gone. And the collapse of the high-tech bubble had transformed the industry that emerged from AT&T's breakup. The Baby Bells were consolidating; long distance was disappearing as a separate business; wireless was displacing land-lines; and the equipment companies that had dominated North America for a century were in trouble. We couldn't just say no when foreign companies came courting. In that context, mitigation agreements became a way to say yes to globalization without completely surrendering to foreign espionage. The agreements became a kind of company-specific network security regulation. We began to insist on a mitigation agreement in any transaction that posed even a modest threat. Each agreement created an ad hoc regime designed to curb foreign government infiltration of U.S. telecommunications and information technology. . . .
>
> [A] common security measure was to insist that the government (or an approved third party with technical skills) be guaranteed the right to inspect the buyer's hardware designs and processes, its software source code and testing results, and any other part of the production process that might reveal a deliberate compromise. To make sure that data was not shipped abroad and compromised there, some mitigation agreements required that data about Americans be kept in the country; sometimes the agreements required special security measures for the data….

> We were acutely aware that these measures weren't perfect. … In theory, access to source code and hardware designs would allow our experts to find any Trojan horse built into the product. But few government workers have the expertise to find these needles in a haystack of products. Unless we insisted that the companies pay for very expensive outside experts to check their work, or we received an intelligence tip about corporate misbehavior, we had only a modest chance of catching a really clever compromise. …
>
> Still, imperfect as they were, mitigation agreements were well ahead of whatever was in second place. They were in fact our only good tool for policing foreign efforts to build insecurity into U.S. networks.

Though there has been progress, it remains true that CFIUS remains one of the few tools that the U.S. government can use to address supply chain risk, especially in telecommunications and information technology.

The mitigation agreements themselves continue to expand in scope as new threats emerge. For example, where it was once enough to insist that telecommunications data and control be kept under U.S. control by maintaining a Network Operating Center in this country, officials have come to recognize that such centers are filled with equipment that must be updated and maintained remotely by the equipment supplier, opening new avenues for compromise. CFIUS agreements now must be concerned not only about foreign companies managing traffic on U.S. networks, but also about the equipment that comprises these networks and the vendors that supply that gear.

But the hard fact remains that CFIUS is an inadequate tool for this job. It gives the government only haphazard insight and leverage over the security of telecommunications and information technology. That's because CFIUS has jurisdiction only over corporate acquisitions. Team Telecom, which I also oversaw from a DHS perspective, adds a bit to that authority, giving national security agencies an ability to impose conditions on foreign telecommunications carriers seeking Federal Communications Commission licenses to operate in the United States. But Team Telecom has no explicit authority in law; its reach is no greater than the FCC's. As a result, even the most dangerous and unreliable suppliers of commercial telecom and IT equipment are free to sell their products in the United States without an inquiry into the security risks the products may pose.

Even recently adopted programs such as federal government subsidies for rural wireless service and "smart grid" deployments – programs embraced in the American Recovery and Reinvestment Act of 2009 – have no statutory provisions to ensure that federal dollars are not spent on equipment that will impair national security. And Section 232 of the Trade Expansion Act of 1962, which allows the President to restrict imports that threaten to impair national security,[1] has never been applied outside the importation context. While news reports indicate

---

[1] 19 U.S.C. § 1862. The Supreme Court has upheld broad use of section 232 to restrict imports. *See Federal Energy Administration v. Algonquin SNG, Inc.*, 426 U.S. 548, 564 (1976) (Section 232 authorizes the President "to take whatever action he deems necessary to adjust

that the Commerce Department successfully dissuaded Sprint from awarding a large contract to Huawei, there may be no statutory basis to do so where the contract does not involve importation of products.

3. A Patchwork Quilt of New Measures

That said, the last few years a growing number of government and private-sector stakeholders have taken action to "harden" the ICT supply chain. It is hard to call the resulting measures anything but a patchwork quilt of remedies. There are no standard or consistent practices, and monitoring and verification tools are limited. Significant gaps continue to exist in U.S. policy, and no single U.S. government agency or organization is responsible for supply chain security. (For a good, recent summary of overall supply chain vulnerabilities, I recommend *Remaking American Security*, prepared by former Gen. John Adams for the Alliance for American Manufacturing.) Federal procurement law and policies in particular are struggling to come to grips with ICT supply chain challenges. Nonetheless, these new measures represent a series of experiments and tentative steps that may yet lead to a more comprehensive approach.

Securing Critical Infrastructure

The vast majority of critical infrastructure is privately owned and operated. These owners generally are free to use whatever vendors and supply chains they prefer. Securing government systems is hard enough, but how are we to secure supply chains for privately owned critical infrastructure? This is among the hardest of the hard problems.

A cybersecurity Executive Order issued in February of this year is a decent start. It calls for the development of a cybersecurity framework that critical infrastructure and other U.S. companies will be encouraged or required to adopt.

Due to be published in February 2014, the framework likely will create a basis for official communications discouraging the use of products from untrusted sources and from service providers who depend on such sources. For example, the framework likely will encourage companies to adopt procedures to vet vendors and suppliers from the perspective of cybersecurity risk.

Because large swaths of the U.S. economy are critical infrastructure – including many energy, telecommunications, and transportation companies – this guidance could have a broad impact.

While the Framework likely will not impose mandatory requirements or exclude particular vendors, they may create a mechanism by which security warnings are incorporated into private company security practices. With the Framework in place, critical infrastructure owners are less likely to ignore government warnings about relying on untrustworthy foreign

---

imports . . . [including the use of] tariffs, quotas, import taxes or other methods of import restriction.") (*quoting* 101 Cong. Rec. 5299 (1955) (statement of Sen. Millikin)).

telecommunications equipment providers. If a telecommunications network fails, and calls or emails are disrupted for an extended period of time, the telecommunications company may have to defend the "reasonableness" of its actions in court. If that company ignored government warnings by purchasing untrustworthy equipment, that defense would be a steep, uphill struggle. And that prospect should cause infrastructure owners to heed government warnings.

Government Contracts

Considerable attention has been focused on the threat that untrustworthy products pose for government procurements. The Department of Defense (DoD) has made the most explicit effort to address ICT supply chain security risks by incorporating cybersecurity requirements into acquisition planning and contract administration. Similarly, the National Institute for Standards and Technology (NIST)—which sets information government-wide security standards— has instructed agencies to develop acquisition policies to protect against supply chain threats.

The point of these efforts is to protect mission-critical components, whether hardware, software, or firmware. Suggested protective measures include: (1) withholding the ultimate purpose of a technology by using blind or filtered buys, so that the vendor does not know how the components will be used; (2) additional vetting of the processes and security practices of subordinate suppliers; and (3) restricting purchases from specific suppliers or countries.

To implement this guidance, agencies have begun training contracting officers on cybersecurity requirements and inserting clauses into procurement documents that allow them to disqualify bidders because of supply chain and other security concerns. Going forward, this trend is likely to change the ways in which the government, and its contractors, source procurements.

Much of the focus on government procurement practices has been driven by Congress. For example, Section 852 of the 2012 National Defense Authorization Act (NDAA) requires DoD to map the supply chain for critical items from raw material to final products. The legislation also requires DoD to perform a risk assessment of the supply chain for such items. The FY11 NDAA permits DoD to exclude a particular source that presents an unacceptable level of supply chain risk, and withhold certain information regarding the basis of that decision. The FY12 Intelligence Authorization Act allows members of the intelligence community to do the same.

Recently, a number of congressional hearings and reports, and in some cases specific statutory language, have highlighted the ICT supply chain risk from China in particular and led to a strengthening of restrictions on Chinese products. To take one example, Section 516 of the FY2013 Continuing Resolution bans the Departments of Justice and Commerce, NASA, and National Science Foundation from acquiring IT systems "produced, manufactured or assembled by one or more entities that are owned, directed or subsidized by the People's Republic of China." This prohibition, though not yet implemented, represents a significant change in the IT procurement process, and it raises the likelihood that similar prohibitions could be imposed throughout the federal government.

Indeed, similar bills are pending. The Deter Cyber Theft Act, for instance, would require the Director of National Intelligence to produce an annual report that lists which foreign countries conduct cyber espionage against American companies or individuals, as well as technologies

targeted by cyber spies. Additionally, the bill would require the president to block imports of products containing technology siphoned from the United States.

4. Recommendations

Virtually everyone recognizes that this ICT supply chain security problem is hard and that the "solutions" to date have been ad hoc. Nevertheless, both government and private-sector stakeholders appear to have agreed on a number of common best practices. These include:

- Prioritizing efforts to secure the most important and sensitive systems (especially National Security Systems);
- Use of procurement tools to drive security improvements;
- Use of intelligence community assessments to inform mitigation strategies;
- Development of standards drawn from actual commercial practice wherever possible;
- Finding ways for the government to share specific and contextual threat information; and
- Using technical tools and engineering solutions to mitigate risk.

Of these six common elements, three seem to me to be especially significant for government policymaking (via legislation and/or otherwise). At a minimum, we should consider legislation or executive action encouraging:

1. The use of procurement tools, especially by writing additional supply chain security requirements into procurement contracts, and educating procurement officials about which contracts need these requirements.

The need for supply chain security does not apply just to DoD and security agencies. Many agencies – and private companies – need better information about the provenance of the products that they rely upon. More government agencies should require that contractors and subcontractors develop and submit supply chain security plans that include ICT supply chain specific risk assessments. This will both help prioritize security measures and ensure these measures are consistent with a cost-effective approach. As a guiding principle, the security mechanisms should be more robust depending on the sensitivity of the system, component, or information at issue.

At a minimum, the government should implement mandatory supply chain security training and education for contracting officers and other procurement officials. Without such comprehensive and routine training, government officials will be ill-equipped to adequately understand and evaluate supply chain risk with respect to individual contract vehicles.

2. Additional reliance on intelligence community assessments regarding supply chain risks, with some mechanism to share that information with U.S. Government contractors and other critical infrastructure providers, as warranted, without fear of endless litigation.

The DNI's Office of the National Counterintelligence Executive (NCIX) has developed a common methodology for conducting threat assessments on entities that do business with the

national security community. These classified assessments should continue to inform supply chain security decisions and they should be shared, as appropriate, with industry partners.

I have discussed this idea over the years with various members of the intelligence community, and it never takes long before I hear some variation of, "We can't do that. If we say something bad about a particular company, we'll get sued." If Congress wants to encourage better sharing of threat information, it should devote less attention to the problem of clearances for private sector companies, which I think has largely been solved, and more attention to the problem of how to protect sources and methods while also creating a limited, effective remedy for companies that believe that they have been treated wrongly in a threat assessment.

3. Incorporating technical protections and redundancies into products and systems exposed to supply chain risks.

For some information system components, especially hardware, technical means are available to determine if components have been subjected to tampering. There are also trusted/controlled distribution, delivery, and warehousing options, such as requiring tamper-evident packaging of information system components. The government should look to industry for these solutions and incorporate them into best practices guidance.

Beyond these patches, the federal government may need authority to take action to stop an urgent national security threat relating to the compromise of our supply chain. The embarrassing spectacle of one part of the U.S. government subsidizing small carriers' purchases of foreign equipment at the same time that it is warning large U.S. carriers not to buy the same equipment suggests that we simply do not yet have sufficient legal authority to respond to supply chain threat outside of the CFIUS context.