Sam Crooks
Network Design Engineer
<a cloud service provider>

My background is that I have worked in the gaming (as in casinos, gambling), credit card processing industries, consumer credit and related financial services, currently, I work for a large cloud service provider.

There are a few key areas related to cybersecurity that I'd like to discuss:

1) secure supply chain and tamper resistant compute unit
2) trusted network, resilient against large scale Denial of Service attacks
3) validation program for cybersecurity of cloud service provider services to customers
4) process and workflow for validation that systems meet published security controls
5) security clearance programs for infrastructure systems operation and information sharing purposes
6) exposure of the private sector and general public to actual cybersecurity attacks
7) reference architecture

1) NIST SP 800-53 rev4 draft introduces a variety of security controls related to securing the supply chain against malicious insiders, or similar actors inserting malicious code which may be executed to compromise system security of a computing system. There are several issues which should be addressed to help improve supply chain security.

Some portions of the private sector have been under sustained cyberattack since before 'cyber' was a term used to describe the activity. Other areas of the private sector still have no idea the extent to which a computing system or embedded computer in a device may be compromised by malicious code. Even when it is explained, managers making decisions regarding funding and priority do not have the technical software engineering/computer science background to understand just how simple it is to inject code into a machine through a variety, of attack vectors, and then to subvert a Von Neumann architecture system to cause the malicious code to be run.

The gaming industry, as in slot machines, and related slot accounting systems monitoring them, have been under sustained cyberattack, including the manufacturing and supply chain levels, for more than

30 years. The Nevada Gaming Control Board, and similar private testing labs such as GLI and BMM, which operate on a sort of trusted, accredited authority for those states not as mature in these gaming functions as Nevada, have done a great deal to combat the supply chain threats to the gaming industry. The progress made in the gaming industry has been through rigorous technical testing, publication of approved and revoked code levels, rigorous validation and certification, and ongoing continuous monitoring of how this this certified, attested, validated state is maintained, enforced by serious penalties (including suspension and revocation of licensing required to continue to operate in the industry). The measures have included maintaining a published list of excluded persons barred from working in or around the industry, as well as development of detailed standards and processes to validate and certify initial and ongoing adherence to these standards.

Other industries have had to adopt similar measures (banking, finance, securities, credit card processing). NIST has done a creditable job outlining the broad technical requirements in long form (455 pages in 800-53 rev4).

*** Additional work is needed ***

a) One issue with portions of the private sector is lack of understanding and visibility to the threat, particularly those outside of financial sector and related monetary attacks by criminals. A public clearing house of declassified/published information (suitably obfuscated as to intelligence/disclosure source), disclosing in detail, discovered supply chain cyberattacks, would help to begin to address the lack of understanding of the threat in many parts of the private sector. Similar to the National Vulnerability Database (NVD), a database disclosing details about attacks.

b) a program for validation and certification to particular levels that a computing system has controls preventing supply chain compromise. What I am talking about is a program similar to the CVMP program for FIPS 140-2, Levels 1 - 4. A standard and then a process to certify the system design and initial validated configuration state will eventually be required for computing systems supporting designated critical infrastructure.

c) tools to automate the validation that a particular system and all related embedded system are running approved, cryptographically certified firmware, and that they are in the approved configuration state. Automation tools built by NIST or DHS, leveraging the work done in the DoD with SCAPs and "STIGing" a system to validate the state would be a good start, with them made available in binary and source format as a free reference implementation to any and all who want the information. This could help 'seed' the marketplace for these tools to achieve the end goal for the government with NIST 800-53 rev 4, as well as spur adoption in the private sector.

d) a free, reference implementation of Continuous Monitoring automation tools, in binary and source code, made available to the public. These appear to be in alpha/beta PoC stage based on work presented by parts of the Dept of Homeland Security S&T directorate, with parts of the Dept of State systems being used to prove that Continuous Monitoring provides better outcomes than FISMA "point in time" checkpoint processes. Making these tools available to the public will do a great deal to help raise the bar for cybersecurity for the rest of the government and the private sector critical infrastructure areas.

2) Recently there was the largest ever, sustained Distributed Denial of Service (DDoS) attack, against Spamhaus. This attack was so large that it was not able to be accurately measured. DDoS attacks have been in use since the early 2000's timeframe as a means of extortion of payments by criminals against credit card processors and others. The 95th percentile billing model is the generally accepted and implemented means of fairly determining the bill which a customer should pay an Internet Service Provider for Internet transit services. Under the 95th percentile billing model, a company has 96 hours of maximum utilization of their ISP links which will be discarded as being above the 95th percentile. After that point, the company has the dilemma of financial ruin through sustained high bandwidth bills or of disconnection from the Internet. Only the largest networks can even begin to survive a typical DDoS attack today, which is say 20 Gbps sustained. Outside of Cloud and Internet Service Providers, few companies have any need for anywhere near this level of Internet connectivity.

The Federal government has a great deal of Internet capacity for its TICs, MTIPS connections for those departments not authorized to run TICs, as well as the DoD IAPs, when it is all summed together. The nature of how the federal government procures network WAN services from 5 GSA awarded Networx vendors, with each agency contracting for services separately effectively shatters this large Internet capacity into small pieces of capacity. The disaggregation of capacity then exposes agencies to DDoS attack. Building a Federal WAN as a DWDM optical network built between critical Federal interconnection points, and extended to commercial Internet exchange points, with open peering to any and all networks who wish to peer directly to the Federal network, would do a great deal to improve the ability of the Federal agencies to have the scalable capacity, built cost effectively, to sustain very large DDoS attacks.

If the network was then additionally a 6VPE MPLS VPN network on fiber that the Federal government owned or at least has 20 yr IRUs to use, operated as a shared infrastructure facility by an internal agency with a maintenance contract issued to a private company to operate it (like federal buildings, the DoE sites, and countless other examples), the majority of the WAN transport for those agencies using it for their WAN connectivity between data centers, main offices and egress points would be on a network which can scale in bandwidth nearly infinitely (DWDM over fiber gives this ability), which aggregates Internet and private capacity (while maintaining isolation between agencies), and the critical traffic transit points within agency networks (between users and their data centers) can be monitored by sensors providing this information to DHS, US-CERT and FNS. If such a network were built among the data centers being consolidated out of and into by the Federal government as part of the FDCCI initiative, the end result is that the FDCCI would be accomplished more cost effectively and at accelerated rates.

If the network is 6VPE (MPLS VPN for IPV6), then the result is that large parts of the WAN transport will be IPv6 enabled much sooner than will reasonably occur with the 5 Networx vendors, and the end state will be a monitored, more secure, much more cost effective IPv6 ready network, able to sustain existing cyberattack levels and grow cost effectively to sustain them in the future.

If the federal government were to sponsor an entity to operate and manage a similar design for the Critical Infrastructure sector (similar to ARIN or ICANN), as a sort of MPLS VPN enabled distributed Critical Infrastructure Exchange model (similar to the IXP model which resulted from the Federal Internet Exchange (FIX) in 1989, and which helped to initiated the private growth of the Internet), where designated Critical Infrastructure entities could become members and connect to each other for scalable connectivity, monitored by US-CERT for cyberattacks and intrusions, the result would be more protected and scalable infrastructure, with monitoring of it by US-CERT to be able to more broadly correlate cyberattacks on US critical infrastructure in addition to the federal government networks.

3) FedRAMP is a great start to certification of cloud services as meeting a minimum bar. The main problem with FedRAMP is that it is a consolidation of legacy (paper) processes. FedRAMP should be considered an initial implementation. DHS, NIST and the GSA FedRAMP program should over time provide the reference implementations of tools and SCAPs to automate the collection and validation of system compliance, and incentivize CSPs to use them or build/buy their own validated versions, to improve the FedRAMP cycle time and get further toward an end state target of continuous monitoring and a workflow where approval of new code deployments can be validated on an ongoing basis.

4) Cybersecurity could be improved by making the source code available to the government through a system where access to the code is logged, authenticated and exposed such that code may be viewed by read-only users through an interface which permits access one source file at a time, but which prevents mass download and theft of intellectual property. If access is authenticated and identity cryptographically validated (through a system like the Trusted Identities in Cyberspace, and better, if code check-ins for critical systems are also cryptographically signed and validated, tracked by an identity which follows the developer through their career. Such a system would provide the ability to statistically identify who checks in code which is later found to have security flaws or malicious code, and access to the source code by security researchers to validate a security flaw and accelerate the confirmation and resolution of the security flaws can be improved. Pattern analysis (Big Data) will over time identify where malicious code or flawed code with security issues is coming from.

5) In offering cloud services to government and defense sector, there is presently a sponsorship of N clearances per customer. In addition, different government agencies will have different clearances required than other government agencies in a different sector.   For example DoD has Secret, Top Secret, TS/SCI. DoE has L and Q clearances. Other agencies have a similar background investigation requirements, PTP-Low, PTP-Med and PTP-High. For the private sector, there are background checks but not really an approved "clearance" for working in a private sector critical infrastructure function. It would help government, as well as the private sector critical infrastructure companies, if there were an equivalence of clearances within the government established so that a cloud service provider does not have to have staff go through multiple background checks and investigations for different parts of the government. A general "Critical Infrastructure Sector" clearance scheme for offering services to Federal, state and local governments, as well as other Critical Infrastructure sector companies is needed.

6) Education of the private sector and general public. This could be aided by exposure of the public to details of the threats and methods. Case Studies and walkthroughs of past cyber attacks, and in particular, how these have occurred in the pat by compromising the engineering, manufacturing and supply chains. Much of the general public and private sector are totally ignorant that there is a field called "supply chain hygiene" and has trouble believing there is a need. This is due, in part, to lack of training as an electrical engineer, computer engineer, or software engineer and therefore a lack of understanding of how computers work at a very low level, and how they may then be compromised, coupled with a lack of real, officially disclosed and publicized information about case studies and examples of actual threats uncovered and attacks which resulted. Exposure will help eliminate disbelief and denial that this is an issue more important to address than other priorities.

7) Publication of an example or reference architecture and program draft by DHS, NIST and FedRAMP of compliant system designs and operational and audit processes would go a long way toward helping to remove the ambiguity and steer the private sector toward better practices. Any time there is an audit, an auditor and a document describing requirements, there is ambiguity and interpretation to contend with. PCI/DSS does a good job of stating the intent and broad goals, and providing detail and supplemental information which helps system engineers and process and program implementers to put in place a system. The Federal standards are lengthy, spread over multiple documents and written such that an agency may pick and choose which controls and issues they require to be addressed today and which are more critical for later days. While this flexibility sounds good, too much choice leads to too much ambiguity and too much interpretation of what is require, desired and not acceptable. A detailed example of a minimum, reference system design and related processes, an unacceptable system and an exceptional system would greatly help in guiding the private sector toward better cybersecurity.