Testimony
Mary Ann Davidson
Chief Security Officer
Oracle

Chairwoman Clark, members of the Subcommittee, my name is Mary Ann Davidson, and I am Chief Security Officer for Oracle. For more than 30 years, information security has been a central part of Oracle's software DNA, and is a big reason why the federal government is Oracle's largest customer. Thank you for the opportunity to testify regarding the important issue of cybersecurity.

1. The Declaration of Independence states "All men are created equal." All information systems, however, are not.

This truth of this statement should be self-evident but it isn't, and therein lies a risk to our freedoms. The ubiquity, flexibility, and configurability of information systems has led to circumstances in which software designed for a particular purpose and environment is too often deployed in an environment it was never designed for, without any thought or explicit acceptance of the risks in so doing. Without properly scoping our requirements we are faced with an all or nothing approach to cyberspace, simultaneously putting at risk our civil liberties, our homeland security and the women and men of our armed forces.

Let me give you a present-day example: I had a most frightening conversation with a highly placed official in the Defense Department who said that DoD wanted to use popular social networking software and that (direct quote) "you in industry need to secure it." My response to that statement: "What is DoD going to use the software FOR? 'Hi, I'm an Al Qaeda operative. I like long walks on the beach and IEDs. Will friend me?'" Without an appropriate context, I noted to the gentleman, there is no magic security dust we in industry can sprinkle on technology that is already "out there and being used," especially if we do not know what it is being used *for*. Certainly there are legitimate scenarios where we may want to permit our troops to use social networking software as a morale booster, including contact with their family and friends, but the technical and policy-based security requirements around that use case are different from a use case where the DoD might use similar technology for operational purposes.

There is no substitute for knowing upfront what you need software for, how it is going to be deployed, and what risks you can accept and what risks you won't. The time to make those determinations is during procurement, not after. The Navy does not purchase container ships and try to deploy them as aircrafts carriers. Nor does the Air Force purchase Gulfstream Vs and try to configure them as F-22 Raptors. There is nothing wrong with container ships or Gulfstream Vs, by the way, but they were not designed for the operational needs or – and I emphasize this last point – threat environment that aircraft carriers and F-22s were designed for. Why, then, is information technology somehow "different?" It isn't. Private industry and government agencies have varying

use cases and threat environments in cyberspace, just as they share different requirements in the real world. And where privately run information systems can benefit from defensive technologies informed by our offensive capabilities – to use a metaphor - this rising tide will lift all ships in cyberspace.

Unfortunately, many think software is so flexible and configurable, that one size fits all applications. It doesn't. The military already knows this, but sometimes they need an occasional reminder. When I was a naval officer, I had many different uniforms: dress blues, dress whites, tropical whites, khakis and utility greens. Each had its purpose. Should one be foolish enough to wear dress blues to a firefight, it isn't merely that you will be breaking uniform regulations; you aren't going to be adequately protected, either. You wear body armor to a firefight. While cost is one consideration in deployment, it need not be the only one, unless we plan on digging up old Lee-Enfield rifles and giving them to the Marine Corps instead of the M-16s they now use. "You get what you pay for" is as true in software as in anything else.

Good security, like good hardware starts in procurement: knowing what you need, how it will be used, and explicitly describing the threat environment for deployment. Use procurement wisely and aggressively.

This brings me to my second point.

2. Information technology is mission critical, not merely mission enabling.

Our entire economy rests on an IT backbone: the acronym "IT" therefore represents "infrastructure technology" as much as "information technology." In particular, our homeland security and our military's ability to prosecute war rests on an IT backbone. DoD continues to invest in network centric operations, which is all about getting the right information to the right warrior at the right time in the right battlespace. Therefore, the network itself **is** the battlefield because the network is what our enemies will attack if they want to deny us the ability to use our own technology (or in an attempt to use our technology against us).

Given that DoD has bet the farm on information systems, they need to enhance its treatment of information systems as a core mission specialty in supporting roles as well as using information systems offensively as a warfare specialty. Absent this capability, the DoD will not able to fully use IT as the force multiplier it can be. Just as Patton knew his tanks *and their technical capabilities* very well, not just merely how to deploy them, our military and homeland security leaders need to know and embrace the full capability of IT. Putting it differently, do we envision having a contractor at the helm of an in-theatre aircraft carrier? If not, then why would our cyber offense be any different? Note that the ability to deploy and support systems itself is also a critical mission specialty, just as, say, supply/logistics is a staff function in the military but a critical one. Patton knew very well that Armies stop without supplies of gas; information or net-centric armies stop without supporting information systems. Furthermore, only by holding capability for both functions in esteem can "offense inform defense" and vice versa.

We must also remember the strength of the American economy rests on the flexibility afforded the private sector to innovate and market those innovations globally. In the same way our nation's electrical grid, pipelines, roads and railways support our military but are not run by our military, our critical cyber infrastructures and the companies who create them cannot simply fall under military control. Of course our government should defend our cyber interests, but in the same way we would abhor a military presence at every intersection, we must also ensure civilian control over the normal operation of our digital highways.

This brings me to my third point:

3. We are in a conflict – some would say a war. Let's call it what it is.

Given the diversity of potentially hostile entities building cadres of cyberwarriors, probing our systems for weaknesses, infiltrating U.S. government networks and making similar attempts against American businesses and critical industries – including our defense systems –is there any other conclusion to be reached? Whatever term we use, there are three obvious outgrowths from the above statement. One is that you do can't win a "conflict" – or war - if you don't admit you are in one. The second is that nobody wins on defense. And the third is that we need a doctrine for how we intercede in cyberspace that covers both offense and defense and maps to things we value in the real world. In short, Congress should consider developing a 21st century application of the Monroe Doctrine. The need for a framework to guide the government's role in response to foreign aggression is a point that Melissa Hathaway has already noted during her 60-day interagency review of the Federal cybersecurity mission, and an area where this subcommittee can productively collaborate with the National Security Council.

For those a tad rusty on their US history, the Monroe Doctrine (introduced December 2, 1823) said that further efforts by European governments to interfere with states in the Americas – the Western hemisphere – would be viewed by the US as acts of aggression and the US would intervene. The Monroe Doctrine is one of our longest standing foreign policy tenets: invoked on multiple occasions by multiple presidents, including Teddy Roosevelt, Calvin Coolidge, Herbert Hoover and John Kennedy. We have, as the expression goes, sent in the Marines - and the rest of our armed forces - to support the Monroe Doctrine.

Note that the Monroe Doctrine did not detail the same intervention or even specific intervention for each perceived act of aggression, merely laid out "here is our turf; stay out or face the consequences" language that allowed great flexibility in terms of potential responses. Some may argue that cyberspace is "virtual" and unsuited to declared spheres of influence. But even Internet protocol (IP) addresses map to physical devices in physical locations we care about – critical infrastructures such as a server for a utility company in New York, for example, or a bank in California.

The advantages of invoking a Monroe-like Doctrine in cyberspace would be to put the world on notice that the US has cyber "turf," (properly scoped - we should not claim all cyberspace as our turf - there is plenty to go around). And the second is that we will defend our turf. We need to do both. Now.

As I mentioned earlier, having a military response capability does not mean militarizing all elements of U.S. cyberspace any more than invoking the Monroe Doctrine meant necessarily creating permanent encampments throughout the Western hemisphere. Nor should a cyber-Monroe Doctrine lead to permanent government encampments in private networks. With proper guidance, various government agencies and the private sector can find their natural role in guarding our cyber infrastructures in a manner similar to how we currently protect our real-world interests.

To summarize

- Technology is only a force multiplier if you pick the right technology for the intended use **and intended threat environment**. The government must make security an explicit part of procurement, funding appropriately skilled staff to execute these procurement requirements while recognizing that some non-commercial requirements will incur additional costs.
- We need a skilled cadre of government information technology professionals – both offense (in the military) and defense (throughout the government).
- We need the cyber-equivalent of the Monroe Doctrine for our 21st century information age that respects the boundaries of our shared ownership of the nation's cyber infrastructure.