Remarks to the U.S. Senate Committee On Commerce, Science, and Transportation
of Mary Ann Davidson
Chief Security Officer, Oracle Corporation
February 23, 2010

Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee, I am Mary Ann Davidson, Chief Security Officer for Oracle. I appreciate the opportunity to appear before you today, and I also want to commend the committee for tackling the issue of cyber security – it's a very tough and multi-faceted issue. I also want to thank the committee for including industry in the drafting process of cyber security legislation, partnership between government and the private sector is critical for making our public infrastructure safe and secure.

When many of us were young, we looked up to superheroes: Superman, Batman, Aquaman and Wonder Woman: the people who could do almost anything and were unstoppable (except – perhaps - by Kryptonite). When we grow up, most of us realized that there are no superheroes: many problems are very difficult to solve and require a lot of hard work by a lot of smart people to fix. So it is with the security of critical infrastructure: we cannot shine a signal in the sky and expect SuperNerd to come and save us.

Many intelligent people have proposed a number of ways we can help define the problem of critical infrastructure protection as it relates to cybersecurity, "bound" the problem space and improve it. There are two specific recommendations that may help stem the problems of the present and change the dynamics of the future: both are necessary to help secure not only today's but tomorrow's critical cyberinfrastructure.

First, we need to change our collective mindset so that elements of critical cyber infrastructure are designed, developed and delivered to be secure. We do that in part by changing the educational system so that we have a cadre of people who *know* that critical cyber infrastructure will be attacked - and they build accordingly and defensively. We do not generally think of the New Testament as a guide to critical infrastructure protection, yet consider the parable of the builders, in which Jesus contrasts the man who built his house on rock with "…a foolish man who built his house on sand. The rain came down, the streams rose, and the winds blew and beat against that house, and it fell with a great crash" (Matthew 7:24-27). This parable is an apt description of the problems in securing critical infrastructure: if our infrastructure "builders" do not understand the difference between building on rock and building on sand, our house will collapse in the first good rainstorm.

The second recommendation is more straightforward: we need to stop "upping the ante" on exposing critical infrastructure to - in some cases - unknowable risk - and we should walk away from the gambling tables until we both understand the odds *and* the odds are better. What we know now is that we continue to expose critical infrastructure to the Internet in the interests of saving money, which massively increases our attack surface, we do not, in many cases, know how exposed we are, and we have determined enemies. "Doubling down" is not a strategy – except a strategy for catastrophic loss.

Changing the Educational System

One of many cybersecurity risks the Department of Defense is concerned with involves the supply chain of software – more specifically, the risk that someone, somewhere will put something both bad and undetectable in computer code that will allow enemies to attack us more easily. However, that is but *one* type of supply chain risk we should worry about and perhaps not even the most critical one. In fact, "the software supply chain" at a fundamental level includes the people who design, code and build software. We should worry about the supply chain of *people* as much or more than the supply chain of software itself, because those who design, code and build software don't know how to build it securely and the institutions – with some notable exceptions – who educate them either don't know or do not care to know how woefully inadequate their educational programs are. (Some universities, of course, do care about security and have invested in improving their computer science curricula accordingly. Kudos to them.)

If we were having a rash of bridge failures, and we discovered that universities were failing to teach structural engineering to civil engineers, we would not be discussing how to redesign tollbooths and train tollbooth operators, or teach people how to drive safely on bridges. Similarly, proposals to "certify more cybersecurity professionals" is only a remedy for the cyber threats to critical infrastructure if we understand the problem certifications attempt to solve and ensure that we focus on the *right set of professionals to certify*. This is especially true since "cybersecurity professionals" these days may well include Chad, the 12-year-old who installs anti-virus on his technophobic grandparents' computer.

Several years ago Oracle sent letters to the top 10 or 12 universities we recruit from[1] – more specifically, to the chair of the computer science (CS) (or equivalent) department and the dean of the school in which the computer science department resided - telling them that:

a) We spent millions of dollars fixing avoidable, preventable coding errors in software that lead to exploitable security vulnerabilities;
b) We have to train CS graduates in how to write secure code because they were not taught these skills in computer science programs;
c) We need universities to change their curricula to address this clear and present educational deficiency; and
d) The security of commercial software has become a national security issue.

Oracle received precisely one response to these letters, and that was a request for money to enable that university to create a "secure programming class." In the last six months, a representative that same university – at a Department of Homeland Security Software Assurance Forum no less – said publicly (and in apparent reference to the Oracle letter) that his institutions' graduates were "too good" for vendors like Oracle.

[1] A heavily redacted form of this letter is available at http://www.oracle.com/security/docs/mary-ann-letter.pdf and a larger discussion of the supply chain "personnel" issue is available at http://blogs.oracle.com/maryanndavidson/2008/04/the_supply_chain_problem.html

It's hard to imagine a more tone-deaf response to a "customer" request for a better "product. "

Some have proposed that we certify "cybersecurity professionals" to improve the protection of our critical infrastructure. However, certifying cybersecurity professionals – presuming we could define the term precisely enough to avoid certifying absolutely everybody who touches an information technology (IT)-based system – is too late in the game. You can't secure something that was not designed to be secure or that has holes big enough to drive the QEII through. Putting it differently, in the physical world, do we certify interior decorators or the people who build the house? It's architects, engineers and contractors who are professionally licensed, not the people who move furniture around and pick out color schemes. (No disrespect to security administrators – or interior designers - is intended by this comparison; the fact remains that cybersecurity professionals cannot necessarily secure a system that was not designed to be secure.)

In the physical world, engineering degree programs are accredited and engineering is a profession. Engineering graduates take the engineer-in-training (EIT) exam – proof that they learned and absorbed basic engineering principles in their degree program as part of their career progression. Most who choose to actually practice the engineering profession must become a licensed professional engineer (PE). While it is true – as many academics are quick to point out – that we understand the physics of, say, bridge design, and there are – as yet – no "physics" of computer systems, that does not mean that we should not expect people who are being educated in computer science to know both what we know now, and what we do not know: specifically, how to think about complexity and risk. At any rate, the fact that Oracle and other large software vendors almost universally must teach the basics of computer security to computer science graduates building IT-based infrastructure should give all of us pause.

We know that embedding sound principles in curricula and reinforcing those principles throughout a degree program works: this is why physics is a "core" course for engineers and why civil engineers cannot conveniently ignore physics in upper level classes. We also know that an increasing number of professions involve computers and thus the need for "security" - embedded and reinforced throughout a number of curricula and a number of classes within those curricula - is critical. Control system design, for example, absolutely must include an awareness of sound security principles or we will merely repeat the mistakes we have already made. And yet, too many universities continue to fiddle while Rome burns, or at least, fiddle while Rome is hacked.

A modest proposal in pursuit of curricula change would be to link government research funding to phased educational reform in computer and computer-related degree programs. That is, cutting off all money until the curricula is fixed is counterproductive (as it penalizes institutions that actually are making positive changes even if they are not "there" yet). But we can certainly demand that universities submit a plan to alter their curricula that includes specific delivery dates for curricula change and insist that they make those changes as delivered – or else. Currently, there is no forcing function to change education. Many university professors are tenured and thus have no incentive to

"cure." One of the few market forces we can exert is money – such as grant money. If parents can tell their toddlers that they don't get any dessert until they eat their peas, the US Government can certainly tie research funds to phased curricula change.

There are two additional reasons to – immediately and with some urgency – forcefully impose curricula change on the universities that deliver the pipeline of people building critical cyber-infrastructure. The first is that we are already out of time: when the Soviet Union launched Sputnik, it lit up the skies and lit up our eyes. The US rapidly moved to dramatically improve the science and technology focus of our educational system so that we, too, could conquer space. As regards cybersecurity, we have already had our Sputnik moment: in fact, we in cybersecurity have such moments over and over, every single day. The most damning comment one could make about the recent Google-China headlines is that for those of us in industry, it was merely the exclamation point on a long narrative, not an opening soliloquy.

The second reason is that everybody is looking for expertise to secure what we have today – not to mention, what we are building in our headlong rush to site critical infrastructure upon technical "sand." For example, the Department of Homeland Security has stated that they want to hire 1000 cybersecurity professionals.[2] Where will they find them? The military is standing up cyber commands[3] and it seems increasingly obvious that wars of the future will increasingly take place in the cyber realm. Where are these future attackers and defenders to come from?

In particular, the military views technology as a force multiplier and their information systems increasingly form the background of their ability to fight wars. What possible confidence can the military have that the network elements on which they base their ability to prosecute war can be trusted if the people who built them do not understand at a very basic level that all software can and will be attacked? The people designing and building software do not, in general, think, design and code defensively because they are not educated to do it. We might as well be turning out Marines who don't know that they have enemies, or what a firefight is or what "take the hill" means. The results would be and are predictable. Marines are lethal in no small part because they know there are enemies, and they train to annihilate them.

Slow Our Exposure to Systemic Risk

There is an old saying that goes, "quit while you are behind, and when you are in a hole, don't dig." Nowhere is this truth more evident than in our rush to increase the interconnectedness of critical infrastructure and its exposure to the Internet – an exposure that creates risks that we do not understand and thus cannot mitigate. We embrace the interconnectedness because the benefits – and cost savings – seem clear, but the risks are murky. No sensible person, of course, should say that we cannot do *anything* that involves risk. Life is about assuming risk.

[2] http://www.cnn.com/2009/POLITICS/10/02/dhs.cybersecurity.jobs/index.html
[3] http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=222600639

That said, and as a cautionary tale of assuming risks we do not understand, we need look no further than the recent financial system meltdown in which massive computer programs could quantify all kinds of risk *except* the most important one: systemic risk. The financial superheroes "in charge" and the brilliant "quants" that were their super-sidekicks got it wrong. Nobody really knew the degree to which entity A was exposed to entity B and what would happen if the thread between them was snipped. It turns out; systemic financial risk was the Kryptonite that brought down Superman.

Alas, a lot of technophiles pushing new "problems" we need sophisticated IT-based solutions for, or those eagerly embracing new uses (and abuses) of technology, do not realize that everything – including technology – has limits. The "limits" are not necessarily those of bandwidth, or protocols we haven't invented yet. The most important limitation is our inability to make rational, informed decisions about risk because of complexities we simply cannot fathom.

In the many discussions on what the government can do to fix cybersecurity, including "spend more money on research," and "certify cybersecurity professionals," it is worth noting that no single proposal will "save us," and certainly not any time soon. There is, however, one thing we can do today: stop making cybersecurity worse by rushing to use technology in ways we know very well we cannot secure and that create huge systemic, unknown (and thus unmitigateable) risk.

One such area is smart grid. The general idea, we are told, is to allow power plants to a) get lots of near-real time measurements on power consumption (e.g., from your house) to better price power consumption accordingly and b) do remote maintenance of grid elements (e.g., deployed in your house). If we can do better demand pricing we can build fewer plants and be "smarter" about power usage. Nobody is necessarily opposed to "do more with less" premises, with one big caveat: what if the "more" is "more risk" – a lot more? More, in fact, than we can fathom. What we know about smart grid should – if not scare us – at least induce a very large gulp:

- We already know we cannot secure millions of Internet protocol (IP)-based clients: it's hard enough to secure servers. The millions of PCs that have been co-opted into botnets are proof enough of that.

- We know that the SCADA (Supervisory Control and Data Acquisition) protocols used in control systems were not designed to be attack resistant: they were originally used in electro-mechanical systems where you had to physically access the control to use it (i.e., turn the knob).

- We know people are increasingly moving to Internet protocol (IP)-based control systems, and connecting them to corporate networks that are, in turn, connected to the Internet. We thus know that people can access controls for things they shouldn't be able to from places they aren't supposed to be able to. [4]

[4] http://www.c4-security.com/The%20Dark%20Side%20of%20the%20Smart%20Grid%20-%20Smart%20Meters%20%28in%29Security.pdf

- We know that many of the smart grid devices that have already been deployed are hackable.[5] For example, a prototype worm developed by a security research firm was able - in a simulated attack - to spread from meter to meter to take out power in more than 15,000 homes in 24 hours. [6]

- We know that terrorists are increasingly interested in targeting utility grids and in developing their hacking expertise to be able to do so. [7]

- We know that smart grid concepts are also starting to be implemented in gas and water utilities.

- We know that people have built personal digital assistants (PDAs) that "talk SCADA" because "it's so expensive to send a technician to the plant." (It won't be long before we hear: "Move the control rods in and out of the reactor? There's an app for that!" Some day we may have a power plant meltdown when all someone was trying to do is answer the phone.)

- And, lastly, we know that the people designing and building these systems were never taught "secure/defensive programming" any more than computer programmers were.

What we can infer from all the above is that the rush to "save money" is being done by people who fundamentally do not understand that they are vastly increasing the potential risk of a cyber attack that can be launched from any home. Against the grid itself. In a way that we do not know how to mitigate. In an increasingly hostile world. If we think saving money on critical infrastructure is more important than protecting it we might as well start sending the Marines into combat with slingshots (so much cheaper than M16s) and expecting them to secure our nation. Neither is acceptable, and both will involve needless and senseless loss of life.

Before we keep trying to "do more with less," let's take a deep breath, step back and think seriously about worst cases and how we avoid them in the first place. *Hoping* our enemies won't exploit a big shiny new attack vector once we've deployed is not a strategy. Actually minimizing the attack surface *is.*

There are a couple of things we can do to slow the lemming-like rush over the smart grid cliff. One of them is to insist on some standards (through existing standard setting bodies) – if not actual certification – of smart grid components. NIST, for example, has led a Cyber Security Working Group that recently released a second draft of "Smart Grid Cyber Security Strategy and Requirements" document.[8] It's a start

[5] http://rdist.root.org/2010/02/15/reverse-engineering-a-smart-meter/
[6] http://www.wired.com/threatlevel/2009/10/smartgrid
[7] http://www.scmagazineus.com/critical-condition-utility-infrastructure/article/161689/
[8] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/NISTIR7628Feb2010

Second, we need a better transparency around how "smart grid" components are built, and *of what* they are built – given a lot of the underlying components may be commercial software that was not necessarily designed for the threat environment in which it will be deployed. It will also help those building critical infrastructure to know how robust the "building materials" are. There are existing mechanisms that can help establish that transparency, such as the Common Criteria (International Standards Organization (ISO)-15408) and the Department of Homeland Security (DHS) materials on improving software assurance in acquisition. [9]

Without knowing how software was built, and what care was and was not taken in development – we are building a house from components we know nothing about and hoping the resultant structure is sound. It isn't merely that a house built on sand cannot stand, it's that a house built of ice won't survive in the tropics and a house built of some types of wood won't survive in a termite-friendly environment. Without knowing what components are being used in the house, how they were designed and built – and with what assumptions – we have no idea whether even a house built on rock is going to stick around for the long haul. There are, after all, earthquake zones.

It may seem difficult to change the status quo, and yet we have to believe in the capacity for positive change – even if that embraces a clear and abrupt departure from the status quo. As the prophet Isaiah said, "Whether you turn to the right or to the left, your ears will hear a voice behind you, saying, 'This is the way; walk in it.' Then you will defile your idols overlaid with silver and your images covered with gold; you will throw them away … and say to them, 'Away with you!'" So be it.

[9] https://buildsecurityin.us-cert.gov/swa/downloads/SwA_in_Acquisition_102208.pdf