



Statement of

Mary Ann Davidson
Chief Security Officer
Oracle Corporation

Before the

Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
Committee on Government Reform

US House of Representatives

17 September 2003

Mr. Chairman, Ranking Member Clay, my name is Mary Ann Davidson, and I am the Chief Security Officer of Oracle Corporation. On behalf of Oracle, I appreciate the opportunity to be here today to offer Oracle's perspective on information security, and specifically, the Common Criteria. This is a critically important topic, especially given events over the past month.

Oracle is the world leader in enterprise software, and is uniquely qualified to comment on information assurance policies. We have spent 25 years building information management systems for customers that I affectionately call 'the paranoids,' which include US intelligence agencies and the Department of Defense. To gain and maintain the business of the most security-conscious customers on the planet, Oracle has made an extraordinary investment in information assurance, and we have 17 independent security evaluations to show for it. The basis of our marketing campaign "Unbreakable" is this long-term commitment to information assurance.

We made this investment in security for one simple reason: Our customers asked for it. They asked for it, and they meant it. Up until recently, we have witnessed what I could call a merry-go-round on information assurance within the federal government. Despite more than ten years of well-intentioned efforts by federal agencies to ask software vendors to have their products independently evaluated, vendors simply refused to do them because, in the end, they counted on the federal government to not follow through on its own request. Meanwhile, the federal government would refuse to get serious about evaluations because not enough vendors did them. A lazy vendor too often was just a weasel-willed procurement officer away from cheating on evaluations.

The collective impact of Code Red, Blaster and Sobe to our economy, which amounts to billions of dollars in repairs and downtime, have worked to send all of us a sobering message: It's time to get off the merry-go-round once and for all. The benefits go beyond more than just secure federal information systems. A strong federal information assurance policy has the potential to change the entire software industry for the better.

Fortunately, some federal agencies are listening. The message has come largely from the policy directive mentioned numerous times already today: NSTISSP #11. This policy, as well as several enforcement components, most notably Department of Defense Directive 8500.1, drew a constructive, clear, pro-security line in the sand. Simply put, for national security systems, an agency can only purchase commercial software that has been independently evaluated under the Common Criteria or the Federal Information Processing Standards (FIPS) Cryptomodule Validation Program (CMVP).

Mr. Chairman, the question before us is not whether NSTISSP #11 makes sense or not. We've had that debate. It's over. NSTISSP #11 is already making a positive, constructive difference in software development. Instead, the question before us is how to make this policy work as effectively as possible and within as many federal agencies as possible.

As we all know, the success of NSTISSP #11 is linked in part to vendors participating in the Common Criteria, the de facto worldwide evaluation standard, which has the added benefit of mutual recognition by many countries, including the US, the UK, Germany, Canada, France, Australia and New Zealand. Vendors complete one security evaluation that is valid in many countries. Consumers of the software have assurance that the vendor is not blowing smoke, because it is someone other than the vendor validating security claims. (Let's face it, all vendors claim they are secure, even the ones who issue security patches for their products every 2 ½ days.) By being linked to the Common Criteria, NSTISSP #11 has three key results:

- First, more secure products. Evaluators find security vulnerabilities, which must be fixed. No fix, no evaluation certificate, no exceptions.
- Second, a more secure development process. Evaluations actually test the process more than the product itself. Product security architecture, functional, design, and test specifications are reviewed, and a secure development process has to be repeatable. Security can only be built in from inception, not “bolted on” after the fact.
- Third, a stronger culture of security. Instituting evaluations as part of software development, and then repeating them over and over changes the corporate culture. Security becomes part of the corporate “DNA,” woven into the fabric of the organization. This is the biggest long-term benefit of security evaluations, because over time, it becomes an industry culture.

It's been 14 months since NSTISSP #11 has gone into effect, and we have seen several very positive developments. First, a number of firms, including several of our competitors, are getting their products evaluated under FIPS or the Common Criteria, and some for the first time. Second, we're seeing firms, including Oracle, financing evaluations of open source products, which will work to dispense some of the myths surrounding the so-called inherent vulnerabilities in open source operating systems. Third, several industry organizations, such as the financial services industry, are coming together to make security a purchasing criterion industry wide and are using NSTISSP #11 as a model.

We're seeing all of this because the initial impression from an industry perspective is that the federal government means business this time. That, in and of itself, is a major victory and credit goes to the people within the Defense Department and intelligence agencies, as well as Congress, who are making a concerted effort to make this process work. The fundamental question for them, you and other policy leaders, and all of us in the security world is how can we continue to make this process work even better. Let me provide a few suggestions:

First, maintain eternal, but pragmatic, vigilance. Enforcement of NSTISSP #11 should be consistent, with no waivers. Fortunately, the enforcement process was set up to discourage waivers, and shifts waiver authority from procurement officers to the

Committee on National Security Systems within the NSA, which was the entity that first developed NSTISSP #11. The merry-go-round that I referenced earlier was driven by a decade of procurement “dodge and weave” via waivers. Last year, in testimony before the House Readiness Subcommittee, I said that when it comes to information assurance, it was time for the federal government to “chirp or get off the twig.” So far, so good. The cat hasn’t eaten the canary yet.

Don’t get me wrong. Several agencies or sub-agencies wouldn’t mind getting off the twig, and opt out of NSTISSP #11. A general sentiment of “NSTISSP #11 does not apply to us,” especially when so many components used by intelligence agencies are standard commercial software and hardware products, sends a terrible message to the marketplace and negates the intent of NSTISSP #11. What could be more central to national security than intelligence?

Second, the federal government should extend NSTISSP #11 beyond traditional national security systems. The creation of the Department of Homeland Security, coupled with the increasing importance of federal government information systems to maintain the effective administration of health care, social welfare and law enforcement requires the entire federal government to make security a factor in software buying decisions. Earlier this year, the President’s National Strategy to Secure Cyberspace recommended a study on the application of NSTISSP #11 across the entire federal government. I encourage this subcommittee to check on the status of this study, work to see it is completed and ensure that representatives of industry have the opportunity to make recommendations. Last year, while debating the creation of the Department of Homeland Security, several Senators, including the former Chair of the Senate Government Affairs Committee, agreed that the new Department should examine how NSTISSP #11 can be implemented in their own procurement policies. I also would encourage this subcommittee to call on the Department of Homeland Security to institute such a policy.

Third, to make NSTISSP #11 work across the federal space, protection profiles should not become agency-centric wish lists. As you well know, Mr. Chairman, evaluations are not cheap. In order to ensure vendors get maximum return on their evaluation investment, evaluated products need to be commercially viable. We have seen protection profiles specifying requirements that no commercial product can meet or for which there is no commercial requirement. If a federal agency wants something new and different, the correct vehicle should be something other than a protection profile. Oracle supports such industry-government dialogues, but the corollary to ‘if you build it, we will buy it’ needs to be ‘can this be built, or is there a better way of solving the problem?’ This often puts us at odds with security purists who design things that are so secure they are undeployable. Fortezza, for example, was never widely-deployed and was given a rousing thumbs’ down by the commercial marketplace, as well as many DoD customers who were supposed to use it. The marketplace ultimately delivered commercially viable encryption, and FIPS evaluations can ensure that the implementations are done correctly.

Similarly, I would recommend that if a federal protection profile effectively requires a Common Criteria evaluation level above EAL4, or imposes a requirement that is not commercially viable, the federal government should pony up the money for the evaluation. Again, the goal here is to make sure that vendors get the investment return. The key commercial advantage of the Common Criteria is mutual recognition -- one evaluation works typically for all nations that are signatories of the Common Criteria Mutual Recognition Agreement. Specifically, at an EAL4 assurance level, mutual recognition applies; at higher levels or at hybrid levels (EAL4 plus some other requirements), mutual recognition is void. Most vendors are willing to do one evaluation — which can run as much as \$1 million per product — as the cost of doing business with the federal government, but a situation where agency specific protection profiles result in “three evaluations per product” is cost-prohibitive. We've been down this road before. Oracle has evaluated products against the US Trusted Computer Systems Evaluation Criteria (TCSEC or “Orange Book”), the UK Information Technology Security Evaluation Criteria (ITSEC), and the Russian Federation Criteria to meet per-country evaluation requirements. We would propose that any procurements requiring assurance levels higher than EAL4 or which void mutual recognition must foot the bill for the evaluation as part of the procurement, including vendor personnel costs. EAL4 assurance is attainable by commercial software products; anything higher is generally non-commercially viable and the procurement officials should expect to pay for a custom solution and a custom evaluation, and budget accordingly.

I know the Chairman has expressed previously his concerns about the cost of security evaluations. Streamlining the protection profile process to prevent unnecessary evaluations can reduce costs, and maintain the commercial viability of the product, without compromising the security benefits of the Common Criteria.

Fourth, country independence of laboratories should be maintained. For business reasons, Oracle’s security evaluation group is headquartered in the United Kingdom and we almost always use evaluation laboratories in the United Kingdom. The process has been wildly successful, with seventeen evaluation certificates under our belt. NSTISSP #11 avoids a nation-centric approach to labs, especially given the obvious benefits to vendors of the mutual recognition provisions of the Common Criteria. That said, we still experience resistance from procurement officers to “foreign” evaluations. This is nonsense. The Common Criteria supports mutual recognition, and a non-US laboratory can become certified to perform (US) FIPS-140 certifications. Also, the Common Criteria process works from objective evaluation standards, and labs, regardless of location, must meet objective standards to become a Common Criteria evaluation facility. Thus, there is slim reason to suspect foreign labs.

We cannot return to the days of country-specific evaluations, which will be the end result if procurement resistance to foreign evaluations spirals down into a policy requirement. We certainly support efforts to make US labs a competitive alternative to foreign-based labs, which would help reduce evaluation costs in the long run. Competence knows no national boundaries; neither does incompetence.

Fifth, the federal government should establish a clearinghouse on evaluation

product information. There are already several good web sites to help both vendors and their federal customers understand Common Criteria, FIPS, and NSTISSP #11.

However, we find that what many of our customers need is a one stop, 'go to' site in order to validate vendor security claims and compare them to the evaluation results themselves. It would be useful for a procurement officer to be able to see all evaluations of any type, for a single vendor, at a single glance, from a single location, whether FIPS-140 or Common Criteria, whether evaluated here or abroad. This empowers them to make apples to apples comparisons. For example, two database vendors can both receive an EAL4 certification, even though one database vendor made two functionality claims in a security target, while the other database vendor made forty security claims. A clearinghouse would enable a procurement officer to perform security target 'scorecarding' and facilitate this and other types of comparisons.

Mr. Chairman, there are no security magic bullets, and certainly, NSTISSP#11 is not meant to be one. What it does provide is assurance that the allegedly secure gun does what its seller says it does, without misfiring and killing the user. The stakes have never been higher for information security, and especially information assurance.

The fundamental lesson of the last 14 months is clear: if the federal government acts like a buyer concerned about the inherent security of its software, its sheer market presence alone will change the behavior of vendors for the better. That said, are there other ways, other than NSTISSP #11, that can accomplish the same purpose? We believe one measure worth considering is for the federal government to insist that the commercial software it buys is either defaulted to a secure setting right out of the box, or made easy for the customer to change security settings. OMB, working in conjunction with the National Institute of Standards and Technology (NIST) and private industry, can specify what is the appropriate default security setting for the software it buys.

We also can't emphasize enough the value of independent research. Assurance is not only evaluations, and even with a good development process, "to err is human." A developer can check 20 of 21 conditions, and if failure to check the 21st causes a buffer overflow, the system is still potentially vulnerable. Hackers only need to find one error, while developers have to anticipate and close every one. It's an uneven battle. The federal government, working with academia, has the ability to jump start research that moves the security ball down the field. One area that deserves attention, especially as more and more US firms partner with foreign countries on software development, is research on effective tools that can scan software and pinpoint irregularities or backdoors in the code. While one would think there would be a market for such software, the research and development involved is seen as cost prohibitive for the private sector. Fortunately, Congress last year passed the Cyber Security Research and Development Act, which authorizes funds for projects like code-scanning tools.

If the medical community could eradicate smallpox with a strong investment in research, we should be able to eradicate buffer overflows.

Finally, industry can do more voluntarily, and in conjunction with academia, to establish professional standards for security officers – professional standards that would evolve as security practices and software development evolved. The software industry also should come together voluntarily to establish the software equivalent of the Underwriters Laboratory. Security evaluations under the Common Criteria are not necessarily cost effective for many forms of consumer software, especially given a price of hundreds of thousands of dollars per evaluation for large, complex products at relatively high levels of assurance. Again, the fundamental goal is to make all commercial software secure by default. To get there, the federal government should work with private industry to establish a consumer software equivalent of the Underwriters Laboratory (UL). Thanks to the UL, most consumer products are generally difficult to operate in an insecure fashion. For example, Cuisinarts are designed so that you can't lose a finger while the blades are whirling. We don't expect the consumer to do anything special to operate Cuisinarts securely; they just are secure.

Far too much commercial software today is built without attention to information assurance principles, leaving many of our national cyber-assets easily vulnerable to an attack. With advanced hacking tools easier to obtain, and the global economy's increasing dependence on web-based platforms to perform everything from financial management to intelligence gathering and analysis, we can no longer patch our way to better security. Instead, we need to move toward a different approach, culture if you will, in which all software sold in the commercial marketplace is secure by default.

NSTISSP #11, DoD 8500.1, and the President's National Strategy to Secure Cyberspace are all welcome developments, because a common theme in all of these documents is the ability of the federal government to use its unique resources on the side of those who adhere to the 'secure by default' culture. I believe we have turned a corner, but it took ten years, and numerous sobering events to get us there. It will take continued vigilance, and continued leadership here in Congress and the Administration to keep us on this road.

Thank you again, Mr. Chairman, for the opportunity to testify today.