



## For Immediate Release

**Contact:** Clint Kreitner, The Center for Internet Security  
540-459-1861; cell: 540-270-8312

Washington, DC – September 23, 2003 – The Department of Energy (DOE), Department of Homeland Security (DHS), National Security Agency (NSA), General Services Administration (GSA), Defense Information Systems Agency (DISA), and The Center For Internet Security (CIS) announced today the public release of a security configuration benchmark for Oracle Database versions 8i and 9i running on Windows and Unix operating systems. It is available free of charge at [www.cisecurity.org](http://www.cisecurity.org).

The benchmark document is a compilation of more than 250 security installation and security configuration recommendations that were identified through a consensus process involving commercial organizations and federal government agencies, including security specialists from Oracle Corporation. It reflects the input of dozens of experts who voluntarily participated in a development process facilitated by CIS.

CIS is developing an automated scoring tool to accompany the Oracle security benchmark. The tool will analyze a host system and produce a score of 0 through 10, with 10 representing the highest level of conformity with the benchmark. Reports generated by the tool will guide users in making changes to harden the security configuration of the database application. The tool is in the final stages of development testing and will be released to the public when complete.

"At the end of the day - federal employees want assurances that the systems they depend on will provide credible data which is secure. The CIS benchmark for Oracle databases and associated scoring tool strengthens our ability to provide this to our fellow employees and protect our national IT assets," said Karen Evans, Department of Energy Chief Information Officer.

The Oracle database benchmark project was led by Carol Bales, Department of Energy Deputy Associate CIO for Cyber Security.

“The consensus reached by this diverse team of security experts is a tribute to Team Leader Carol Bales and many dedicated team members. Karen Evans and her colleagues at DOE are to be commended for exercising strong leadership of this effort. It is an outstanding example of the type of collaboration envisioned by the National Plan to Secure Cyberspace,” said Clint Kreitner, The Center for Internet Security President and CEO.

"The Department of Homeland Security is extremely pleased about the collaboration among federal agencies and the members of CIS. This consensus security configuration guidance for the Oracle database platform is a fine example of how public - private partnership can meet the challenges of improving cyber security," said Sallie McDonald, DHS Acting Director, Outreach and Awareness, National Cyber Security Division.

“I am delighted to see such a large base of public and private sector users working together with a vendor of commercial software to come to consensus on technical security controls. This achievement makes it possible for Oracle to provide its users with a robust set of default security settings, thereby ensuring a higher level of protection against vulnerabilities when implementing Oracle database applications, said Kreitner.

The Oracle benchmark is intended for use by database administrators in managed enterprise environments. The benchmark security settings are divided into two categories, identified as Level 1 and Level 2.

Administrators with minimal security background can implement the Level 1 settings, because they are not likely to break database or application functionality. They represent a minimum security baseline suggested for most environments. Level 2 recommendations secure the system beyond the minimum baseline level, and are intended for advanced level database administrators who will implement them with consideration to the particular database and application environment. The consensus group recommends that these settings be reviewed to comply with local policy and tested on non-production systems before being deployed.

“Information security is a top priority for Oracle, and we are committed to enabling our customers to build better, more secure software. By providing a tool based on common best practices, this benchmark helps organizations more easily meet the challenge of better securing their IT systems,” said Tim Hoechst, Oracle Corporation Senior Vice President of Technology for Government, Education and Healthcare

### About DOE

The Department of Energy's overarching mission is to advance the national, economic and energy security of the United States; to promote scientific and technological innovation in support of that mission; and to ensure the environmental cleanup of the national nuclear weapons complex. The Department has four strategic goals toward achieving the mission: Defense Strategic Goal: To protect our national security by applying advanced science and nuclear technology to the Nation's defense. Energy Strategic Goal: To protect our national and economic security by promoting a diverse supply of reliable, affordable, and environmentally sound energy. Science Strategic Goal: To protect our national and economic security by providing world-class scientific research capacity and advancing scientific knowledge. Environment Strategic Goal: To protect the environment by providing a responsible resolution to the environmental legacy of the Cold War and by providing for the permanent disposal of the Nation's high-level radioactive waste. For more information log on to [www.energy.gov](http://www.energy.gov).

### About DHS

For more information log on to [www.dhs.gov](http://www.dhs.gov).

### About DISA

The Defense Information Systems Agency (DISA) is a Department of Defense (DOD) leader in network management and security and is responsible for security of the worldwide Defense Information System Network (DISN). DISA has developed and maintains 25 Security Technical Information Guides that detail "best practices" for securing various network devices and computer operating systems. For more information log on to [www.disa.mil](http://www.disa.mil).

### About NSA

The National Security Agency (NSA) has dual missions: to provide foreign signal intelligence and to protect vital U.S. information systems. These missions require that NSA remain at the cutting edge of technology. To meet this challenge, NSA employs highly talented mathematicians, computer scientists, engineers, linguists, signals analysts, and intelligence analysts, and aggressively partners with high-tech industry leaders, to include local businesses. For more information log on to [www.nsa.gov](http://www.nsa.gov).

### About GSA

The General Services Administration (GSA) is a centralized federal procurement and property management agency created by Congress to improve government efficiency and help federal agencies better serve the public. The Federal Computer Incident Response Center (FedCIRC), is a collaborative partnership of computer incident response, security and law enforcement professionals working together to handle computer security incidents and to provide both proactive and reactive security services for the federal government. For more information, log on to [www.gsa.gov](http://www.gsa.gov).

### About CIS

The Center for Internet Security (CIS) helps organizations around the world effectively manage the risks related to information security. CIS provides methods and tools to improve, measure, monitor, and compare the security status of Internet-connected systems and appliances. For more information log on to [www.cisecurity.org](http://www.cisecurity.org).

###