FOR IMMEDIATE RELEASE

Follow up questions:
John Gilligan: jgilligan@gilligangroupinc.com
Jim Lewis: jalewis@csis.org
Alan Paller: apaller@sans.org

Consortium of US Federal Cybersecurity Experts Establishes Baseline Standard of Due Care for Cybersecurity – The Top Twenty Most Critical Controls

Resulting Consensus Audit Guidelines (CAG) put into action the national imperative: "Offense Must Inform Defense"

Washington, D.C. (February 23, 2009) -- A consortium of federal agencies and private organizations today released Version 1.0 of the Consensus Audit Guidelines that define the most critical security controls to protect federal and contractor information and information systems. The draft may be found at www.sans.org/cag; www.gilligangroupinc.com; www.csis.org. The public review period runs through March 23, 2009.

The CAG initiative is part of a larger effort housed at the Center for Strategic and International Studies in Washington DC to advance key recommendations from the CSIS Commission report on Cybersecurity for the 44th Presidency.

A "No Brainer"

Cyber attack and defense experts from the federal agencies most involved in cybersecurity pooled their knowledge of the attack techniques being used against the government and the defense industrial base to determine the twenty key actions (called security "controls") that organizations must take if they hope to block or mitigate known attacks and attacks that can be reasonably expected in the near term. They tested their proposal for protecting federal systems to determine whether they would also stop or mitigate attacks known to be used against financial institutions and found the Top Twenty Controls are essentially identical across government, the defense industrial base, financial institutions and retailers.

For each of the 20 controls, the experts identified specific (actual) attacks that the control stops or mitigates, illuminated best practices in automating the control (for 15 controls that can be automated) and defined tests that can determine whether each control is effectively implemented. The resulting document is called the **Consensus Audit Guidelines** and, once fully vetted, is expected to become the standard baseline for measuring computer security in organizations that are likely to be under attack.

The CAG project is led by John Gilligan who served as CIO for both the US Air Force and the US Department of Energy and served on the Obama transition team focusing on IT within the Department of Defense and the Intelligence Community. Of this project, Gilligan says, "It is a no brainer. If you know

that attacks are being carried out, you have a responsibility to prioritize your security investments to stop those attacks."

"This is the best example of risk-based security I have ever seen," said Alan Paller, director of research at the SANS Institute. "The team that was brought together represents the nation's most complete understanding of the risk faced by our systems. In the past cybersecurity was driven by people who had no clue of how the attacks are carried out. They created an illusion of security. The CAG will turn that illusion to reality"

Broad adoption of the CAG may lead to agreement on standards for security automation and government-wide procurement of tools that work. The Federal government spends more than $70 billion on information technology each year. Jim Lewis, Director of the CSIS Technology and Public Policy Program says, "Better use of standards and acquisitions authorities are among the most powerful tools the Federal government has to improve cybersecurity and offer a real opportunity for progress."

Background and Participants

The CAG was initiated early in 2008 as a response to the extreme data losses experienced by leading companies in the US defense industrial base (DIB). The defense industrial base is huge and using red teams to find security holes would have taken decades – and would have found only a smattering of the problems. Quicker and more effective would be to build a risk-based standard of due care based on knowledge gained by DoD red teams and forensics experts. Very quickly the participants recognized that the attacks targeting the DIB were nearly identical to those targeting federal agencies (and sensitive organizations in developed and developing countries around the world). The project took on a greater significance and more organizations agreed to get involved. Today, the team that can take credit for the current draft of the Consensus Audit Guide include the following;

- US National Security Agency Red Team and Blue Team
- US Department of Homeland Security, US-CERT
- US DoD Computer Network Defense Architecture Group
- US DoD Joint Task Force – Global Network Operations (JTF-GNO)
- US DoD Defense Cyber Crime Center (DC3)
- US Department of Energy Los Alamos National Lab, and three other National Labs.
- US Department of State, Office of the CISO
- US Air Force
- US Army Research Laboratory
- US Department of Transportation, Office of the CIO
- US Department of Health and Human Services, Office of the CISO
- US Government Accountability Office (GAO)
- MITRE Corporation
- The SANS Institute

- Plus Commercial penetration testing and forensics experts at InGuardians and Mandiant

The technical editor for the Consensus Audit Guidelines is Ed Skoudis, author of both *Malware* and *Counter Hack Reloaded.* Ed has trained more incident handlers and penetration testers, inside and outside government, than any other person and is often called to manage incident handling when major financial institutions or retailers have been breached.

Next Steps

A six-pronged effort is moving the Consensus Audit Guidelines toward broad adoption:

1. Public review: During the next 30 days, security professional around the world will be reviewing the CAG and providing comments. All suggestions for additions will be put through the same filter that made the CAG valuable in the first place: proposed controls must be provably able to stop or mitigate known attacks and the proposer must provide details of relevant real-world attacks. Comments can be made with or without attribution, but nothing gets added to the CAG unless it can be proven to significantly strengthen defense against real attacks.
2. Pilot implementation: Pilots will be conducted in several federal agencies during this year to test the CAG for value and cost compared with what would have been done under the current practices that the agencies use.
3. CIO Council Review: A security committee of the federal CIO Council will be reviewing the CAG to determine how it could be used on a broad basis to focus federal security expenditures.
4. Inspector General Review: A team from the Federal Audit Executive Council will be reviewing the CAG to determine how it might allow auditors to provide reviews that more accurately measure the security of Federal systems.
5. CAG Automation Tools Workshops: A series of workshops will be held in which federal users that have already automated controls identified in the CAG can present the lessons they have learned about what works and why. The result of the workshops will be requirements documents for automation of each of the fifteen controls that can be used by government procurement efforts such as the GSA SmartBuy program and by the DoD Enterprise Systems and Solutions Group to begin government-wide procurement of the necessary technologies.
6. Global validation: During the comment period, the CAG will be closely compared with the audit guides for ISO 2700x, HIPAA, GLB, PCI, and SOX compliance testing to determine whether any of these include controls and tests that do a better job of blocking or mitigating known attacks.

What Are the Controls?

The detailed Consensus Audit Guidelines are posted at www.sans.org/cag along with detailed control descriptions, examples of attacks they stop or mitigate, how to automate them, and how to test them.

Below is the list of control names:

Critical Controls Subject to Automated Measurement and Validation:

1: Inventory of Authorized and Unauthorized Hardware.
2: Inventory of Authorized and Unauthorized Software.
3: Secure Configurations for Hardware and Software For Which Such Configurations Are Available.
4: Secure Configurations of Network Devices Such as Firewalls And Routers.
5: Boundary Defense
6: Maintenance and Analysis of Complete Security Audit Logs
7: Application Software Security
8: Controlled Use of Administrative Privileges
9: Controlled Access Based On Need to Know
10: Continuous Vulnerability Testing and Remediation
11: Dormant Account Monitoring and Control
12: Anti-Malware Defenses
13: Limitation and Control of Ports, Protocols and Services
14: Wireless Device Control
15: Data Leakage Protection

Additional Critical Controls (not directly supported by automated measurement and validation):

16. Secure Network Engineering
17. Red Team Exercises
18. Incident Response Capability
19. Assured Data Back-Ups
20. Security Skills Assessment and Training to Fill Gaps

====== end ======