



HONEYWELL TECHNOLOGY SOLUTIONS INC.

Honeywell Aerospace
Honeywell Technology Solutions Inc.
Honeywell
7000 Columbia Gateway Drive
Columbia, MD 21046
Tel: 843.744.1221
Fax: 843.744.1071
www.honeywell.com/htsi

Honeywell

**A 50-Year Heritage of Experience
Providing Professional and Technical Services**

Honeywell Technology Solutions Inc. provides global technical services by dispatching skilled professionals where and when they are needed.



Value-Based Solutions Tailored to Your Needs



“Do the Right Thing – Every Time, All the Time”

We deliver the best solutions to our customers through our biggest asset – our people. We believe that honest and ethical behavior is imperative to successful operations and future growth. At HTSI, we expect our people to “Do the Right Thing – Every Time, All the Time”. It’s our culture, it’s the way we do business, and it’s our promise to you.

As technology advances, so do methods of cyber attack and exploitation. It takes far more than hardware to defend today’s complex networks. Proper defense requires complex planning, expert implementation, extensive testing, and continual alertness. Constantly evolving methods of attack require real-time responses that involve expert personnel, cutting-edge equipment, and forward-looking techniques that no attempted off-the-shelf solution can fully provide.

At Honeywell, we understand that true security is not found in a piece of hardware or software alone. We have years of experience with evaluating and implementing security measures on thousands of systems. Our people are experts in (and sometimes helped develop) security standards that protect our nation’s most important data systems. We have developed several unique products that increase security and efficiency in Computer Network Defense (CND), Information Assurance (IA), and Certification and Accreditation (C&A). Honeywell puts all this experience at our customers’ service, listens carefully to your needs and ideas, and provides a customized, comprehensive security solution.

Through superior technical support, world-class personnel, and efficient, affordable services, Honeywell provides complete

end-to-end solutions to support present needs and future necessities. We want to put our comprehensive resources for the full spectrum of integrated IA and cybersecurity at your service, and be your innovative partner.

Policy Translation & Training

Honeywell’s policy, procedures, and training services enable compliance with many standard IA policies and procedures, including the following:

- Department of Defense Instruction (DoDI) 8500 series
- NIST 800-53
- ISO 27000 series
- CIS benchmark tools
- Federal Information Security management Act (FISMA)
- Clinger-Cohen Act
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)

This list grows as new policies are put in place. Honeywell applies its expertise not only to ensure your systems are compliant, but to provide needed training to improve an organization’s ability to defend itself.

Auditing

Honeywell’s extensive policy knowledge and expertise in a wide range of technologies enables us to provide auditing services for your systems’ logical, physical, and cultural security. We conduct

site assessments, review processes and documentation, assist with disaster recovery and business-continuity planning, and perform any other services necessary to evaluate a system’s posture and compliance with a given standard.

Certification & Accreditation

Honeywell personnel are authorized to act in several certification capacities:

- Department of Defense Information Assurance C&A Process (DIACAP) developers
- Security Test and Evaluation (ST&E) testers
- Certification Agents (CAs)

Our personnel follow a National Security Agency (NSA)-approved Information Security Assessment Capability Maturity Model (IA-CMM) process, and hold multiple industry credentials. With domain knowledge in National Institute of Standards and Technology (NIST) 800-37, DIACAP, and FISMA regulations, Honeywell can help with flexible and cost-effective C&A. Honeywell personnel maintain expert status for both United States and European Union IA policies.

Remediation

Quickly addressing vulnerabilities is essential. Honeywell performs hardware and operating-system remediations and system hardening to comply with applied standards, including Time Compliant

Network requirements. We also help keep system defenses updated, create security plans, and design Continuity of Operations Plans (COOPs). Our personnel are experienced with tracking and implementing upgrades and patches, and have established processes that help administrators stay ahead of the latest security information about system components. Honeywell can provide you with the tools, personnel, and knowledge to properly secure your systems and help maintain the level of security your organization needs.

Computer Network Defense

What distinguishes Honeywell is the fact that we offer our clients the same solutions we use to protect our own network. We offer CND services such as real-time and retrospective analyses of network security incidents, and as-required forensic analysis using the Honeywell network in response to such incidents. In addition to incident monitoring and response, Honeywell provides proactive vulnerability scanning, cyber-threat intelligence research, proactive malware analysis, and indicator life-cycle management to strengthen the network-security posture of customer assets. By leveraging our own existing resources, Honeywell can provide up-to-the-minute protection and still reduce costs for our customers.

Honeywell Discriminators

People

Honeywell’s greatest asset is our expert workforce. Our highly trained personnel hold hundreds of industry certifications, and have years of experience in IA, security operations, and testing. To expand this knowledge base, HTSI has recently implemented training to encourage innovation and expansion into new technologies. Certifications held by Honeywell personnel include CISSP, CompTIA Security/Server/Linux Plus, CAP, CEH, GIAC, SANS, and CNSS4011-4013. Honeywell’s IA workforce is entirely DoDD 8570 compliant.

Products

Security Operations Center (SOC)

Honeywell’s CND capabilities include SOC operations, network monitoring, incident response, forensic and log analysis, proactive vulnerability scanning, cyber-threat intelligence research, remediation, and reporting. We operate our own Honeywell SOC in Tempe, Arizona, an operation that must deal with the full spectrum of cyber threats on a worldwide scale, to include Insider Threat monitoring and reporting.

HIAT®

After using several industry-standard tools on C&A tasks, Honeywell personnel created a new way to compile and analyze results that significantly reduced the time of analysis and reporting. The Honeywell Information Assurance Tool (HIAT®) compiles and indexes results from industry-standard tools (Gold Disk, eEye Retina, manual checks, etc.) into a single format. The user-friendly interface helps analysts quickly organize and assess results, and generate reports in a wide variety of formats—even a customer-provided template. Using HIAT® reduces the time it takes to complete critical C&A tasks by up to 60%, which has made it an integral piece of our C&A solution.

CSTAR®

Honeywell developed CSTAR® to increase productivity on DIACAP projects. It tracks a system being validated from initial evaluation to post-ATO maintenance. It can rapidly generate multiple reports, and can be easily tailored for specific customers and systems. Because of CSTAR’s ability to aggregate data from multiple systems into a single view, customers can more easily manage risk, schedules, budgets, and effort across entire projects. For a given DIACAP cycle, we estimate that this tool could save over 800 man-hours per year.