UNISYS | Securing Your Tomorrow™

Stealth for Federal NIAP Certification

Federal Cyber Incidents Increase Exponentially Year After Year

As 2016 comes to a close, cybersecurity has easily become one of the most important challenges we face as a nation. While federal agencies have made significant progress toward strengthening their overall cybersecurity posture, the incidence of cyber threats and their level of sophistication are rapidly evolving. According to a report prepared by the Government Accountability Office (GAO) and presented to the President's Commission on Enhancing National Cybersecurity, the number of cyber incidents reported by federal agencies alone rose by over 1,300 percent from 2005 to 2015. In just ten years, the number of cyber incidents at the federal level increased from 5,503 to 77,183.

The National Information Assurance Partnership (NIAP)

To ensure that federal agencies are using trusted products and solutions, the National Information Assurance Partnership (NIAP) was formed to evaluate Commercial Off-The-Shelf (COTS) Information Technology products for conformance with the Common Criteria it set forth. COTS incorporates the NIAP-managed Common Criteria Evaluation and Validation Scheme (CCEVS), a national program for developing protection profiles, evaluation methodologies, and policies that ensure achievable, repeatable, and testable security requirements. In essence, NIAP is focused on providing secure solutions that leverage industry innovation for rapidly evolving government customer requirements across the world. NIAP certification, which represents evaluations of commercial IT products for use in National Security Systems, is recognized by governments in such countries as Australia, Canada, Germany, India, Malaysia, New Zealand, and the United Kingdom. NIAP certification allows government and civilian agencies as well as foreign governments access to some of the most advanced security technology available.

Unisys Stealth Approved to Protect Classified Information Systems

Unisys Stealth® has been evaluated, accredited, and approved by NIAP as one of the products eligible for use by governments in more than 20 countries seeking to protect their most sensitive

and critical systems. This achievement represents independent validation of the work Unisys is doing to meet the security requirements federal agencies and top enterprises demand today, and serves as a stamp of objective quality assurance.

Stealth was also jointly approved by the National Security Agency's (NSA's) Commercial Solutions for Classified (CSfC) program. Housed within NIAP, CSfC helps facilitate the use of commercial products in layered solutions in order to protect classified National Security Systems (NSS) data for U.S. government customers. According to the NSA's Central Security Services Information Assurance Directorate, this CSfC validation makes it possible for U.S. federal agencies to purchase Stealth within composite solutions that protect classified systems and data.

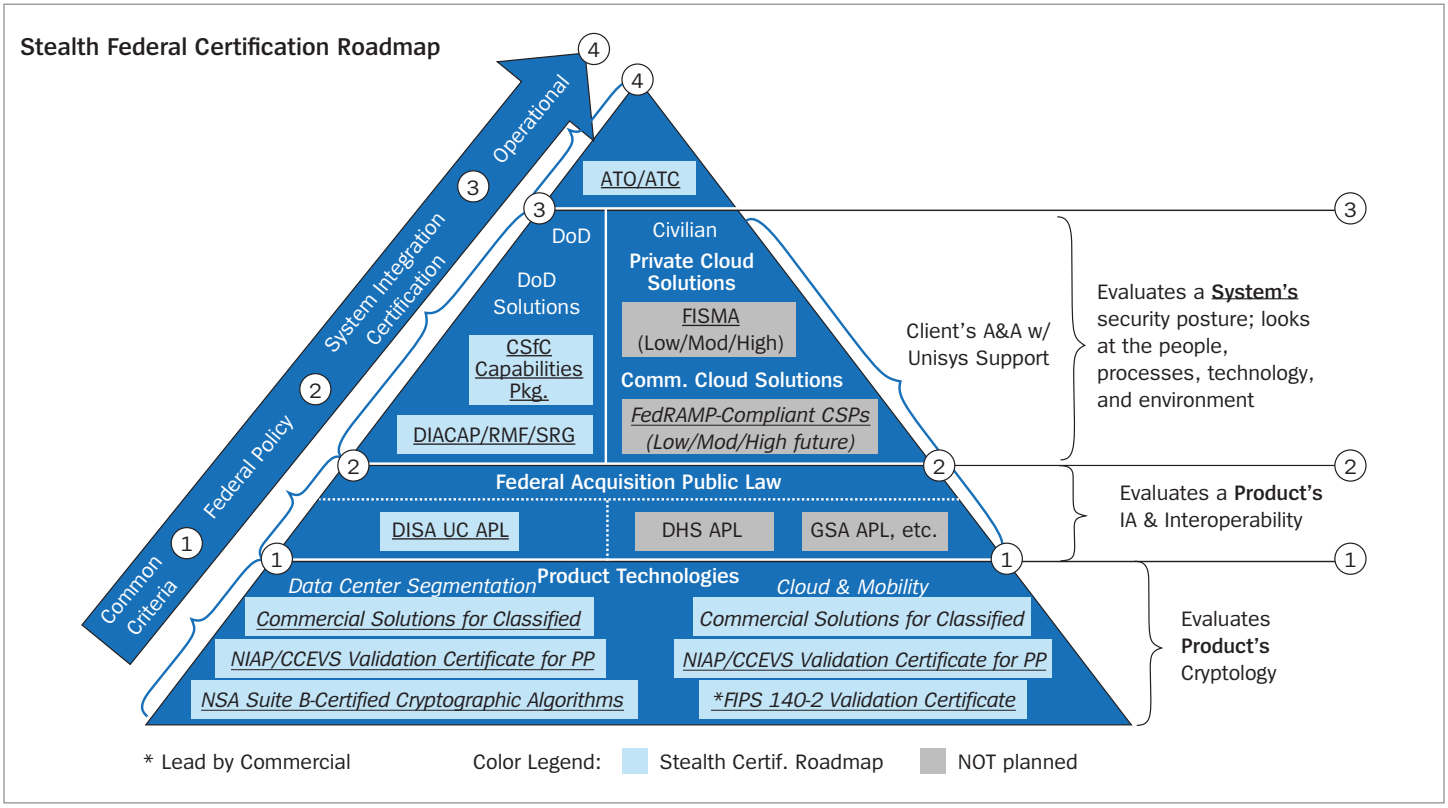
Common Criteria Protection Profiles

For Stealth-protected server and client endpoints, the Stealth software solution is IPSec-based, leveraging the Operating System's (OS's) native IPSec implementation and, hence, that OS's certification(s). Specifically, Stealth is compliant with the IPSec VPN Client Protection Profile for Windows endpoints and is also classified as a CSfC-approved VPN IPSec Client Component.

It is important to note that since October 1, 2009, NIAP/CCEVS policy has changed to accept products into evaluation against NIAP-approved Protection Profiles rather than Evaluation Assurance Levels (EALs). While EALs were largely the *de facto* standard for evaluation prior to this time period, EAL requirements were not achievable, repeatable, and testable in all cases and provided a false label of assurance. Thus, NIAP/CCEVS policy now restricts product evaluations to technology-specific Protection Profiles with achievable, repeatable, and testable requirements and assurance activities. You can see a list of all approved NIAP Protection Profiles here.

Stealth Certification Roadmap

While the Stealth software solution has achieved NIAP/CCEVS certification, the fundamental milestone associated with the product's cryptology, the solution must also achieve three consecutive milestones in order to complete the overall Stealth certification roadmap. However, achieving the first milestone provides the necessary, veritable "credentials" for an organization to feel confident about the product's encryption.



What Sets Stealth Apart

Besides being the only software-based product on NIAP's product compliant list, Stealth is also the only micro-segmentation solution available within the IPSec VPN Client Component Protection Profile list.

Stealth uses an identity-based, micro-segmentation and encryption methodology to create segments within a network. Stealth cryptographically confines user access to a single segment, thus making it impossible for cyber attackers to move laterally within a network. This helps organizations mitigate attacks and hacker incident by rendering devices, data and end users undetectable to networks.

Stealth is a software-defined security solution that effectively:

- Conceals communication endpoints, making them undetectable to all unauthorized parties inside and outside the enterprise
- Defines access by role or identity and not physical location, so security moves with the user or is relative to a system's application environment and is easier to manage
- Protects sensitive data in motion from potential compromise via encryption
- Leverages site-authorization techniques for easy deployment, and enhances it by authorizing users and systems to permit only allowed communication
- Executes inside the enterprise for remote access, from site to site, and incorporates wireless and mobile communications

In addition to these benefits, Stealth adds significant value to the conventional safeguards organizations may already have in place or may be currently considering for achieving or maintaining compliance with industry standards.

Stealth helps organizations sustain compliance with standards in this way:

- Stealth offers one comprehensive technology suite, thereby reducing the need for organizations to deploy multiple products and thus ensuring a more stable environment.
- Stealth simplifies IT administration. Organizations often find that they are unable to sustain compliance with standards over the long-term as a result of the time-consuming modifications they need to make when adding or deleting users or changing privileges. With Stealth, this is a matter of adjusting membership in a Community of Interest without the need for a firewall rule or other physical changes.
- Compliancy technical safeguards tend to evolve to requiring tighter controls and stronger security in more areas of the environment. Stealth inherently provides the capabilities to "lock down" access and communications as tightly as the organization desires and executes on many platforms and profiles (internal, remote access, mobile, wide area).

For more information visit www.unisys.com

Printed in the United States of America 01/17 17-0023