STEALTH

SAIC®

Exclusive Federal Reseller

# A New Era of Remote Government: Unisys Always-On Access™ (AOA), Powered by Stealth™

## Enabling Remote Employees and Government Delivery

Governments are under increasing pressure on multiple fronts to provide remote access to their services and systems. Citizens want on-demand availability to information and assistance. Watchdog groups insist upon transparency and public access to people's data. A changing workforce is pushing for telecommuting options. Now, adding to this pressure, the COVID-19 pandemic is demonstrating how emergencies can disrupt public agencies' efforts to provide help to citizens when they need it most if remote access is not available at need.

The single biggest hurdle to enabling remote government work is information security. Whether referring to personally identifiable information (PII), sensitive government data, or classified material, protecting the transmission and dissemination of information is paramount. The key to such security – especially when working from outside a protected network – is to trust no one. That is the definition of Zero Trust security, which requires the authentication and authorization of a user before granting access to a network.

Zero Trust security is now the recommended defense posture for all IT environments, including government agencies. Zero Trust provides protection for data, applications, and systems regardless of whether employees are on site, at command posts, or working remotely from a home office. With the support of Zero Trust security, operations can continue even during unexpected or emergency situations where entire government business units and functions must be moved offsite, such as with pandemics, terrorist acts, facility failure, etc.

## Preventing Disruption Through a Software-Defined Perimeter and Zero Trust Security

A Zero Trust security defense has always been an elusive goal for government agencies. Infrastructure installations and hardware-defined security systems are expensive to deploy, maintain, and upgrade. They inevitably develop holes that require patching; or, worse, holes that cannot be patched. They are also restrictive, locking an agency into a specific vendor's approach and solution.

Now, however, you can implement Zero Trust security cost-effectively and swiftly with **Unisys Always-On Access™ powered by Stealth™**. Unisys Stealth® establishes a Software-Defined Perimeter (SDP) through identity-based microsegmentation. The SDP serves as the foundation of a Zero Trust security strategy. It simplifies and improves network security even in hybrid/complex IT environments, and replaces the traditional VPN attack surface. You achieve Zero Trust security as Stealth:

- Overlays every corner of your enterprise's computing environment with one holistic, consistent, and unwavering security policy – encompassing desktops, servers, cloud, mobile, kubernetes containers, and IoT
- Enables the creation of cryptographic communities of interest (COIs) that limit access to the other users, applications, and data also assigned to the COI
- Employs hyper-secure IPsec tunnels, leveraging military-grade encryption to strongly protect data from end-to-end

- Provides orchestration and deployment that are highly-automated and centrally-managed so that as your security policies evolve, changes can be made once and propagated instantly across the enterprise
- Monitors and enforces all your Zero Trust security policies, dynamically isolating potential threats and alerting administrators of suspicious behavior

## Swift Deployment of Always on Security

With **Unisys Always-On Access powered by Stealth**, you can retain your entire existing infrastructure and applications. There is no need for an expensive and time-consuming "rip and replace" effort – you can deploy Stealth swiftly and seamlessly, securing your agency with a constantly-updated, easily-upgraded, and never-obsolete SDP.

Through Stealth, your agency can keep operations up and running with secure connectivity, even when employees have to shift to a remote work environment. This is Zero Trust security that is always on, always updated, and never been hacked. This is Zero Trust security designed for you.

**Your Government Agency Will Gain:**

- A more secure alternative to VPNs
- Encryption of data-in-motion to prevent man-in-the-middle attacks
- A reduced attack surface without impeding authorized access
- Operational simplification and increased security through easily-managed COIs
- Protection against data exfiltration
- Accelerated adoption of Zero Trust architecture
- Policy and role-based protections for every user and endpoint on the network

**Learn more about how SAIC can help your agency architect, build, and maintain Zero Trust at www.SAIC.com/stealth and contact us at www.SAIC.com/stealth-contact.**

**SAIC is the exclusive reseller of Unisys Stealth to the federal government.**

For more information visit www.unisys.com