Contract number:
DIR-MSS-SCP-001

Prevent, Detect, & Respond

Texas Department of Information Resources
Statewide Managed Security Services (MSS) Contract

AT&T

“Even a seemingly minor breach can have wide-ranging implications.”

The risk is real.

In a recent survey of state legislators, almost one-third of survey respondents said their state’s cyber risk is high[1]. However, in the same study, far too many underestimated the threat to their systems and data. More than half ranked their cyber risk as moderate or low, while 13 percent responded they didn’t know.

In reality, all government entities hold some type of valuable or sensitive material, whether it is citizen records, financial information or procurement data. Therefore, everyone is a potential target. And in today’s highly interconnected world, each agency—no matter how small—is a stepping stone to another. So even a seemingly minor breach can have wide-ranging implications. The time for action is now.

[1] http://www.governing.com/papers/What-Legislators-Need-to-Know-about-Cybersecurity-8894.html

Prevent, detect & respond.

The Texas Department of Information Resources (DIR) awarded AT&T the DIR-MSS-SCP-001 Contract to offer managed security services statewide. The services include security monitoring and device management, risk and compliance testing, and incident response. We’ve worked with the State of Texas for a decade to help state agencies and institutions address cybersecurity and data privacy issues.

Through this new agreement, AT&T security products are now available to additional state agencies, higher education institutions, cities and counties, special districts and school systems. With AT&T cybersecurity solutions and services, your organization can more securely support its device, application and network operation needs.

AT&T has unparalleled visibility into new and evolving security threats with more than 2,000 security specialists and 8 Security Operations Centers monitored 24/7/365. With more than 186 petabytes of data crossing our network every day, our experts have unique insight into the threat landscape that helps detect new threats before they become a problem. We see more than 90 billion potential vulnerability probes across our global IP network every day. Our integrated suite of cybersecurity tools and technologies help organizations prevent, detect and respond to threats.

Start the conversation today by contacting us at **texasmss@att.com**

Eligible to Texas entities statewide

The comprehensive suite of solutions and services found on the DIR-MSS-SCP-001 Contract include cybersecurity threat monitoring, device management, risk and compliance and incident response. The solutions are also available through the Statewide Technology Center for purchase by other state entities, including **government agencies, cities, counties, K-12 and higher education institutions** across the state. These solutions can be accessed through DIR's marketplace allowing a simplified order and fulfillment process.

The DIR-MSS-SCP-001 Contract comes after the passage of the Texas Cybersecurity Act providing services that will help state agencies meet their legislative mandates.

What's inside

Security Monitoring and Device Management (SMDM)

Every organization needs security intelligence. AT&T security monitoring will provide your entity with the systems, staffing, and analysis required to develop and deliver agile and adaptive Security Information and Event Management (SIEM), Log Management and Analysis, as well as Threat Research services.

In addition to helping protect your organization, additional benefits include the reduction in time, complexity and resources required to actively maintain a highly secure environment.

Every new device on your network is a potential target. AT&T not only manages devices to provide optimal performance but configures each system to deliver optimal data. Providing visibility so that you have the necessary protections to help safeguard your environment from cyberattacks.

AT&T provides device management for:

Firewalls—help prevent unauthorized access into your network[2]

Intrusion Detection and Prevention Services—rapidly identify, block, and respond to network threats

Endpoints—help protect end user computing devices from hazards on the public internet

Web Application Firewalls—controls access to web applications by monitoring and potentially blocking malicious web traffic

To effectively protect against emerging threats it is critical to combine both strong prevention and detection capabilities. The ability to adapt instantly across your infrastructure to help prevent new threats. And then apply newly learned intelligence to detect existing breaches. These capabilities provide an effective means to disrupt the attack killchain and minimize the dwell time of breaches.

[2] The Schools and Libraries (E-rate) Program provides discounts to keep students and library patrons connected to broadband and voice services. To determine if Managed Security Services qualify for e-rate funding, please view the USAC Eligible Services Document at: http://www.usac.org/sl/applicants/beforeyoubegin/eligible-services-list.aspx. For any Managed Security Services that qualify for e-rate funding, customers will use the DIR Service Provider Identification Number (SPIN): 143005581 when filling out forms to request reimbursement for this service.

Incident Response

When your organization is under a cyberattack, rapid and thorough incident response is essential to minimize the threat and safeguard critical systems and data. Time compounds the problem and any delay or inefficiency will only increase the damage and loss from a security breach.

AT&T provides the following incident response solutions:

Security Incident Management—assess incidents, mitigate, and eradicate attacks, provide forensic analysis and manage communication

Digital Forensics—an AT&T led investigation which includes pre-incident preparation, initial detection and response, data collection, data analysis, final analysis and reporting

Response Preparedness—plan proactively to help prevent future security incidents including table top exercises and teambuilding to prepare for detection, response and containment of incidents.

Risk and Compliance

Risk and compliance solutions help to identify, remediate, monitor, and manage risks with penetration testing, vulnerability scanning, policy and process assessments and more.

AT&T provides the following risk and compliance services:

Penetration Testing—testing the organizations security posture by simulating "real world" attack scenarios that include walkthroughs of actual compromises

Risk Assessment—assess policy and process design, architecture, and compliance monitoring

Cloud Compliance—better address evolving regulatory requirements and help protect your organization from growing threats

Vulnerability Scanning—provides an in-depth technical review of your current security posture and proactively identifies vulnerabilities

Web Application Scanning—addresses Internet-facing applications for potential security weaknesses including scanning checks for "open doors" that could allow hackers to gain unauthorized access

Work with a provider that knows government.

Security is at the core of everything we do—our networking, our collaboration tools, our devices, and our cloud services. By bringing together solutions that help protect, serve and connect—committed AT&T professionals are working across the state to identify and implement technology to transform the business of government. With the threat landscape as pervasive and complex as it is, start the conversation today by contacting us at texasmss@att.com.

To learn more about the DIR-MSS-SCP-001 Contract, please visit the Texas Department of Information Resources website.

AT&T