Telos provides advanced technology solutions that empower and protect the worlds most security-conscious enterprises.

- Telos is a start-over vs. a startup. In 1994, began selling off prior businesses to organically re-build as an internet security company with no permanent capital.
- In 2011, published a visionary article extolling the security of the cloud.
- In 2012, sequestration caused us to shift to expand beyond the US government to commercial.
- Today, we deliver security solutions in the areas of cybersecurity, cloud security and enterprise security.
- Developed thousands of work-years of technology and automation to keep our customers more secure.
- Using the security solutions model, we deliver the end result for our customers for a firm fixed price over 80% of the time.
Representative list of Telos Customers

Recipient, James S. Cogswell Award for Outstanding Industrial Security Achievement
Examples of how Telos Security Solutions are used by our Customers

Conducted assessments for and defend the most attacked networks in the world

Xacta® continuous security risk management and compliance automation solution is the database of record for the U.S. Intelligence Community and deployed throughout the US Government

Integrator of record for the largest identity application in the U.S. federal government

Xacta selected by Amazon Web Services (AWS) and Microsoft Azure for cloud compliance solutions

Selected to manage PreCheck enrollment

Deployed our trusted identity vetting application at approximately 100 airports and airlines across the U.S.

Authorized as an FBI Channeler to do real-time fingerprint submissions enabling Trusted Identity as a Service

Telos Automated Message Handling System (AMHS) solution handles all the official message traffic for our customers, military, intelligence and diplomatic missions globally

Telos Ghost provides obfuscation and misattribution capabilities that enable intelligence analysts to track and target adversaries online without being seen
Telos: Security solutions that meet the needs of today’s organizations.

Cybersecurity

Cloud Security

Enterprise Security
<table>
<thead>
<tr>
<th>Cybersecurity</th>
<th>Cloud Security</th>
<th>Enterprise Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Solutions that eliminate attack surfaces and continuously assure the security posture of your organization</td>
<td>Security Solutions for moving systems and applications to the cloud and keeping them secure and compliant in the cloud</td>
<td>Security Solutions and Secure Networks capabilities that support the tactical and strategic goals of today’s enterprises</td>
</tr>
<tr>
<td>• Xacta: cyber risk management and compliance solutions</td>
<td>• Cloud compliance solutions</td>
<td>• Identity management</td>
</tr>
<tr>
<td>• Telos Ghost: Secure anonymous web and network access solutions</td>
<td>• Continuous cloud risk management and security validation</td>
<td>• Organizational messaging</td>
</tr>
<tr>
<td>• Global enterprise security solution deployments</td>
<td>• Assessment, design, and migration solutions to move to the cloud</td>
<td>• Secure mobility solutions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Network management and defense</td>
</tr>
</tbody>
</table>
Cyber risk management, continuous assessment, and ongoing authorization.

Enterprise risk management and data visualization at scale to help you understand and reduce cyber risk across your organization.

<table>
<thead>
<tr>
<th>Security Solutions</th>
<th>Cybersecurity and Cloud Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST RMF</td>
<td>NIST CSF</td>
</tr>
<tr>
<td>NIST SP 800-171</td>
<td>NIST SP 800-53</td>
</tr>
<tr>
<td>RMF for DOD IT</td>
<td>ISO 27001/27002</td>
</tr>
<tr>
<td>CNSS 1253</td>
<td>HIPAA</td>
</tr>
<tr>
<td>FedRAMP</td>
<td>PCI-DSS</td>
</tr>
</tbody>
</table>

*On premises, hybrid and in multiple clouds*
Security Solutions: Cybersecurity and Cloud Security

Xacta

- Xacta is the leading commercial risk management platform across the US government
- Growth in commercial enterprises across the globe
- Deep integrations and partnerships with both Amazon Web Services (AWS) and Microsoft Azure

C2S sponsor asked Telos to automate the security compliance of their instance of the AWS cloud in the same way that we have done on premises
- Xacta implemented in Commercial Cloud Services (C2S) and Secret Commercial Cloud Services (SC2S)
- Dramatically reduced time to receive the permission to operate in the cloud from 2.5 years to 60 days
- New services have been as fast as 7 days
“With Xacta 360’s inheritance and provider project features and capabilities, AWS expects a dramatic increase in efficiencies and effectiveness in completing ATOs, in some cases up to 90% faster.”

Rick Trinidad, World Wide Public Sector, AWS

“Xacta 360 is the solution behind the AWS security assurance team’s compliance support of C2S, reducing our manual effort and ATO times. The automated control update feature in some cases has eliminated four to six weeks of manual effort – per project – each time compliance regulations change.”

Carl J. “CJ” Moses, Deputy CISO, AWS
Xacta: Current and Future Market Opportunities

Current markets:
• U.S. Intelligence Community
• U.S. DOD
• U.S. federal civilian
• State and local government
• Defense industrial base
• Banking, financial services and insurance (BFSI)
• Cloud providers
• Large SaaS providers for various industries and applications

Expansion into new markets:
• Critical Infrastructure
• Universities
• International Governments
• Healthcare
• Retail
Reduce your attack surface, hide your digital exhaust, and disguise your digital identity with obfuscation, encryption, and managed attribution.

You can't exploit what you can't see.
Telos Ghost Capabilities

- Cloaked Services: Encrypted communications, storage and applications
- Private Network Access: Secure, private network in the cloud
- Private Web Access: Anonymous worldwide internet access
Telos Ghost Customer Use Cases

- Threat and competitive analysis
- Sharing sensitive Information
- Protecting from unauthorized internal and external use
- Secure remote office and mobile work interactions
- Conceals who you are on the internet
How Customers Are Using Telos Ghost

<table>
<thead>
<tr>
<th>Customer</th>
<th>Use/Application of Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commercial</td>
<td>Worldwide Investigative and Recovery Services</td>
</tr>
<tr>
<td>Commercial</td>
<td>Supply Chain vulnerability assessment</td>
</tr>
<tr>
<td>Commercial</td>
<td>Web-based Defensive Cyber Operation</td>
</tr>
<tr>
<td>DoD</td>
<td>DoD Cyber Protection Team - Network Protection and Cyber Incident Response</td>
</tr>
<tr>
<td>DoD</td>
<td>Red Team/Penetration Testing - Readiness and Security Inspection Team</td>
</tr>
<tr>
<td>Special Customer</td>
<td>Opensource cyber threat intelligence analysis</td>
</tr>
<tr>
<td>Intelligence</td>
<td>Web-based Cyber Operations &amp; Research</td>
</tr>
<tr>
<td>Intelligence</td>
<td>Worldwide communications and secure file transfer</td>
</tr>
<tr>
<td></td>
<td>Red Team/Penetration Testing</td>
</tr>
<tr>
<td></td>
<td>Cyber Threat Intelligence</td>
</tr>
<tr>
<td></td>
<td>Supply Chain Risk Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Telos Ghost: Current and Future Market Opportunities

**Current markets/Use Cases**
- DoD
- Intelligence Community
- Supply chain security
- Cyber threat intelligence
- Red teaming
- Investigation and recovery services

**Expansion into new markets**
- Law enforcement
- Homeland security/first response
- Financial services
- Healthcare
- Industrial control systems/IoT
- Energy
Security Solutions: Enterprise Security

Identity

DMDC
Military ID
- Integrator of record for largest identity application in the US Government – Military ID (CAC)
- Biometric and Biographic capture and enrollment
- Smart cards
- Two decades of experience and support

FBI
Fingerprint Capture
- SaaS biometric web capture
- Pre-employment screening
- Identity Vetting
- Enrollment and fingerprint capture
- One of only a few companies authorized by the FBI to offer this service

TSA – Airports
Employee Vetting
- Continuous monitoring of airport employees – Security Threat Assessment
- Fingerprint capture and FBI records check
- 100+ significant airports, airlines, general aviation customers to date
- 1 of 3 authorized by TSA to offer this service

PreCheck and Large Health Services Provider
- PreCheck Enrollment Provider – 2M new members per year
- Provider Enrollment contract holder – Background checks for 1.6M healthcare providers each year

Telos ID Advantage
Trusted Marketplace
- Enrollment Services
- Vetting on Demand
- Insider Threat Solutions
- Digital Identity Wallet
- Mobile Identity Solutions
- Cloud-based Identity Solutions
- Access & Authentication
- Identity Infrastructure Support
- Identity Network Security and Operations
Digital Identity Market Potential

The global digital identity solutions market size is projected to grow from USD 13.7 billion in 2019 to USD 30.5 billion by 2024, at a Compound Annual Growth Rate (CAGR) of 17.3% from 2019 to 2024.

• Digital identity addressable market areas
  • Software – Enterprise and mobile-based software tools used to administer identity verification and validation.
  • Services – Professional consulting and implementation services necessary for establishing and implementing identity solutions within enterprises.

• Addressable market verticals
  • Retail
  • Finance
  • Health
  • Transportation
  • Law Enforcement
  • Homeland Security & Defense
Biometrics Market Potential

Biometrics compliance market growth: CAGR of 26% from 2019-2023; $907M in 2018 to $3.1B in 2023 (for GDPR alone)

- Biometric addressable market areas
  - **Software** – *Enterprise and mobile-based* software tools used to administer compliance with GDPR and BIPA laws.
  - **Services** – *Professional* consulting and implementation services necessary for establishing and implementing compliance solutions within enterprises.

- Addressable market verticals
  - Retail
  - Finance
  - Health
  - Transportation
  - Law Enforcement
  - Homeland Security & Defense
Automated Message Handling System (AMHS)

• The gold standard for secure messaging across the US Government
• Operationalizes non-repudiation, so messages are legally binding
• Certified to handle TS/SCI message traffic
• Works on premise and in the cloud in both unclassified and classified environments
AMHS: Current and Future Market Opportunities

Current markets:
- U.S. Department of Defense
- U.S. Intelligence Community
- U.S. Federal Civilian
- Defense Partnerships

Expansion into new markets:
- International governments and agencies across the globe
Secure Networks

Secure Mobility and Network Management and Defense

• Designed and delivered the largest deployment of secure mobile networks to the US Department of Defense

• Deployments in the most difficult environments, enabling our customers to connect to any information source, from anywhere, at any classification level, over any wireless medium, using any device

• Provide managed solutions for operating and defending complex enterprise networks

• Defend networks across the commercial and federal space

• Create offensive capabilities for appropriate customer set in the US government
Solutions for business and government that let you work without concern across and beyond the enterprise.

- **Productivity** — mobile and remote workers have access to enterprise data and applications for faster, better-informed decisions
- **Coverage** — seamless roaming between Wi-Fi and cellular; any medium, any device, anywhere
- **Cost savings** — consolidate multiple capabilities into a single integrated enterprise mobility management solution
- **Efficiency** — simplify the process of updating devices with the most recent version of apps and content
- **Security** — centrally managed security policy ensures that people and information are protected wherever they are
Network Management and Defense

Network management services and solutions for operating, administrating, and defending complex enterprise networks and defensive cyber operations

- **Network operations** — situational awareness of your networks, including users, systems, and security posture
- **Network maintenance** — preventive maintenance, troubleshooting, and repairs
- **Defensive cyber operations** — real-time threat monitoring, analysis, and remediation to ensure continuity of operations
This presentation contains forward-looking statements. For this purpose, any statements contained herein that are not statements of historical fact may be deemed to be forward-looking statements. Without limiting the foregoing, the words “believes,” “anticipates,” “plans,” “expects” and similar expressions are intended to identify forward-looking statements. There are a number of important factors that could cause the Company’s actual results to differ materially from those indicated by such forward-looking statements. These factors include, without limitation, those set forth in the risk factors section included in the Company’s Form 10-K for the year ended December 31, 2019, as filed with the SEC.

Certain information contained in this presentation and statements made orally during this presentation relates to or is based on publications and other data obtained from third-party sources. While we believe these third-party sources to be reliable as of the date of this presentation, we have not independently verified and make no representation as to the adequacy, fairness, accuracy or completeness of, any information obtained from such third-party sources.

This presentation has been prepared solely for information purposes. This presentation is not an offer to sell or a solicitation of an offer to buy securities and is not a solicitation of a proxy, consent, or authorization.
Solutions that empower and protect the enterprise.