TG utilizes an enterprise-wide, cyber-risk management framework, deploying the resources necessary to implement, operate, and sustain a robust cyber security posture. This helps protect corporate data through proven cyber security measures based on technology, personnel, and practices.

TG makes a significant commitment and investment in cyber security, protecting borrower data, including nonpublic personal information (NPI) and personal identifying information (PII). The potential DCS contract as well as last summer's Department of Education (ED) mandate that all FFELP guarantors be Federal Information Security Management Act (FISMA) compliant and adopt the National Institute of Standards and Technology (NIST) security control framework has reinforced TG's cyber security posture.

Technology

TG has made a considerable investment in technology to implement technical controls that provide an automated basis for implementing security and privacy controls.

- **Identification and Authentication** – These technologies enforce identification and authorization controls to assure TG management that only authorized personnel can access our data and processing resources in order to carry out TG business.
    - Software deployed to enforce identification and authorization includes:
        - Top Secret (mainframe)
        - Active Directory (network)
        - LDAP & DB2 (MyTG portal)
    - Application Systems – manages access controls (Artiva, DACCS, and JD Edwards)
    - Two-Factor Authentication – required for remote access and for certain privileged user access within the network (RSA)
    - Network Access Control – only allows known TG devices to connect to the internal network and access TG resources (Cisco)
- **Malicious Software** – Malware is used by various types of attackers to gain unauthorized access to data, networks, applications, and other processing resources. The technologies TG has deployed to protect from this risk are:
    - Anti-Virus, Anti-Spyware – monitors devices for the presence of viruses and other malware and remediates those identified based on known signatures (McAfee)
    - Advanced Malware Protection – detects/blocks malware based on behavioral analysis (FireEye)
    - Web Proxy – controls outbound Internet traffic to protect against visiting malicious websites and other categories of websites (IronPort)
    - Email Gateway – monitors incoming email for known malware

Vulnerability Management – operating system and application software routinely require vendor patches to mitigate identified threats. TG uses technology tools to scan for vulnerabilities and apply patches.

  - Vulnerability scanning – identifies exploitable vulnerabilities, internally and externally (Nessus)
  - Patching tools – patching management software detects where patches are needed and applies them (Shavlik)
  - Configuration management – determines how certain system types should be configured to minimize vulnerabilities within the requirements of supporting operational needs
  - Security Information and Event Monitoring (SIEM) – ingests log files and reports/alerts on specified events
  - Annual network and application penetration testing – utilize a third party, Netspi, to test our Internet-facing presence for vulnerabilities that can demonstrably be exploited

- **Data Protection** – These technologies prevent loss or disclosure of data in the event of lost hardware or attempts to send sensitive data out of our network
  - Laptop HD Encryption – protects data stored on laptop hard drives in case the laptop is lost or stolen (Sophos)
  - Secure USB Ports – USB devices are disabled on all equipment
  - Encrypted email – protects email that contains sensitive data (Cisco Registered Envelope Service)
  - Data Loss Prevention – monitors outgoing data for potential movement of sensitive data if content appears to be SSNs or other NPI (RSA)

Personnel

Our people implement and maintain the processes and technology to manage, monitor, and comply with the framework requirements

- Chief Information Security Officer (CISO) with over 30 years of security experience gained during his tenure with various financial institutions, health care providers, and oil and gas exploration companies
- Dedicated information security staff who hold various certifications and collectively represent nearly 125 years of experience
- Institute of Applied Network Security (IANS), the leading provider of in-depth security insights and decision support delivered through research, community, and consulting is a key resource in keeping the information security staff current on cyber security risks

- Computer Security Incident Response Team (CSIRT) – IT staff organized to respond to detected intrusions on our network

Security Awareness Training Program – TG requires all new hires to receive security awareness training and all personnel to refresh that training annually. Certain departments have additional training requirements as well. Periodic security oriented newsletters and bulletins are published on TG's intranet.

Practices

TG's processes are documented in a well-defined body of information security and privacy related policies, standards, and procedures built with FISMA compliance in mind as well as other regulatory requirements such as the Gramm-Leach Bliley Act (GLBA).

New business initiatives may bring other compliance requirements including Payment Card Industry – Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), and the Health Information Technology for Economic and Clinical Health Act (HITECH).

- **Annual independent FISMA compliance assessments** are conducted by an experienced, well-known cyber security firm, CoalFire
- **ED's initial FISMA compliance assessment** found TG to be an **industry leader** in cyber security
- **Annual Independent Audit** – as a component of their annual financial and compliance audit, KPMG assesses general Information Technology controls, including those related to cyber security.
- **Internal Audit** routinely evaluates various elements of TG's cyber security.
- **Third-Party Vendor Management** – when TG engages external companies to provide services that can impact security and privacy of data and processes, we employ due diligence reviews to determine if the vendor or service provider has sufficient protection mechanisms in place.
- **Business Continuity Planning** – if TG experiences a catastrophic loss of processing ability, we have established business service and infrastructure recovery plans. Additionally, data is backed up, and encrypted, on a defined schedule to facilitate recovery of processing functions in the event of a prolonged outage or unavailability of our facility. Recovery plans are reviewed and updated on a regular basis.