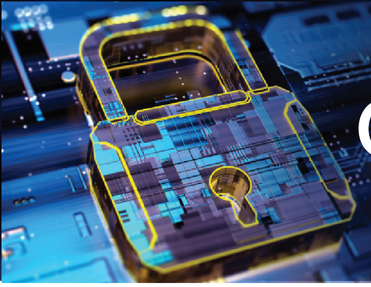

Cybersecurity

Management

OPPENHEIMER

On February 12, 2013, an Executive Order (13636) was issued by the White House regarding “Improving Critical Infrastructure Cybersecurity” in response to repeated cyber intrusions into critical infrastructure. The Executive Order was designed “to assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm...” and deemed applicable to all critical infrastructure sectors.

The Financial Services Industry is regarded as one of the most critical infrastructure sectors. In this regard, Federal agencies such as the Securities and Exchange Commission (SEC), State agencies such as the New York Department of Financial Services, Self-regulatory Organizations such as Financial Industry Regulatory Authority (FINRA), and industry trade groups such as Securities Industry and Financial Markets Association (SIFMA) have all issued Cybersecurity guidance to member Firms. Further, political and economic unions such as the European Union also have developed new regulations for businesses that serve European Union residents. This guidance is focused on strengthening an organization’s Cybersecurity program.

Oppenheimer Holdings, Inc. (including its subsidiaries, “Oppenheimer” or “the Firm”) has taken great strides to consolidate, enhance, manage, and proactively review its Cybersecurity policies, standards, and procedures. It has developed a framework and methodology that voluntarily complies and supports the premise of the Executive Order and other applicable regulations.

Oppenheimer’s Cyber Security program works to protect the privacy information of our clients and protect the confidentiality, integrity, and availability of Oppenheimer’s systems and data. This is done by using a National Institute of Standards and Technology (NITS) based frame work. In fulfilling this, Oppenheimer leverages industry leading tools and does activities such as the following:

- Physical security controls for office space and our data centers
- Annual review and update of our detailed cyber security policy and related procedures
- Mandatory information security training for our workforce several times a year
- Secure coding practice training for our developer community
- Spam, malware, and anti-virus protection
- Data Loss Prevention (DLP)
- Vulnerability scanning/discovery, assessment, and fix
- A Security Information Event Manager (SIEM)
- Secure Messaging
- Application penetration testing
- Firewall penetration testing
- Annual risk assessment and risk management
- A Cyber Security committee that solid line reports to the CISO and the Risk Committee
- Regular cyber security reporting to the Board and Risk Committee
- A Chief Information Security Officer with over 30 years’ experience in cyber security and IT Risk management
- Talented cyber security staff with historically low turnover
- Comprehensive network monitoring
- Network Access Control for blocking unauthorized connections to the network
- End point protection
- A 24X7 Security Operations Center (SOC)
- A 24x7 Network Operations Center (NOC)
- An Incident Response (IR) Team
- Dynamic site scanning and analysis
- DDoS Protection
- User and Entity Behavior Analytics (UEBA)
- Use of encryption on servers, laptops, and mobile devices
- A framework-based Cyber Security policy and metrics-based reporting to validate compliance to the policy
- Finally, Oppenheimer carries cyber security insurance backed by Lloyds of London

Oppenheimer & Co. Inc. Transacts Business on All Principal Exchanges and Member SIPC. 3309084.1
v10.20