FINANCIAL SERVICES Information Sharing and Analysis Center

PRESS RELEASE

FINANCIAL INSTITUTIONS CAN IMPROVE OPERATIONAL CONTINUITY AND REDUCE RISKS ASSOCIATED WITH A DESTRUCTIVE CYBER ATTACK VIA NEW LEADING PRACTICES GUIDE

Reston, VA – 23 NOVEMBER, 2015 – The Financial Services Information Sharing and Analysis Center (FS-ISAC) today announced the availability of a leading practices guide for financial services entities that are working to improve their operational continuity and reduce risks associated with a destructive cyber attack.

A destructive cyber attack is a unique threat in that it is both rare and yet potentially catastrophic. Such an attack can present a significant threat to an organization's daily operations and business continuity; it potentially impacts confidentiality, integrity and availability of data, and can potentially thwart an organization's ability to recover from an attack. An interagency working group comprised of The Financial Services Information Sharing and Analysis Center (FS-ISAC), the National Institute of Standards and Technology (NIST) and other agencies have worked to deliver materials that map the currently available resources for financial institutions.

Bill Nelson, President & CEO, FS-ISAC said: "This important initiative highlights the financial sector's proactive approach to dealing with new risks and emerging threats in order to best protect their enterprises and customers' assets. Recent destructive cyber incidents in the gaming and entertainment sectors illustrate how such an attack can compromise an organization's data integrity, disrupt business operations, and harm brand reputation. While destructive attacks are rare, financial institutions of all sizes should be prepared. We recommend that our members review their existing strategies to protect critical assets and have a complete plan for operational recovery to preserve data integrity against this evolving risk."

Nate Lesser, Deputy Director of the National Cybersecurity Center of Excellence at NIST stated: "When assessing risks, many organizations focus on what data can be stolen and used for profit, like intellectual property or customer records. Threats to data integrity like destructive malware can be overlooked, and reducing the risk of such threats is critical to securing data and information systems. We are excited to be working with FS-ISAC and the broader consumer community to help organizations prepare for, and recover from, attacks that might compromise their data."

NIST defines malware as "a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system." While malware is an umbrella term that include many types of malicious software code, the recommendations in this new guide are focused on malware that destroys the confidentiality, integrity and availability of data. Financial institutions should work to reduce the risks associated

with potential cyber-attacks involving destructive malware. The materials provided by the working group deliver recommendations in the context of the NIST Framework to defend against such an attack attack including the following steps:

Identify – Gain situational awareness by identifying critical data, backup processes and systems in the organization that is necessary for critical business functions, where it comes from, where located, and where used. Having a thorough knowledge of solution components, training, vectors, detection technology, ongoing risk assessments, monitoring, information sharing and incident response keeps the enterprise in a continuous state of alert and prepares an organization to take action promptly.

Protect – From network and endpoint security to system redundancy and backup to reputation management, a variety of controls are necessary for a comprehensive and robust security framework to protect corporate data and personally identifiable information.

Detect - Speed is essential in detecting malware when it enters a key environment, understanding the context, whether it is destructive in nature and quickly assessing the full potential impact.

Respond - In the event of unauthorized access, the financial institution's computer systems could potentially fail, and confidential information could be compromised. Management must decide how to properly protect information systems and confidential data while also maintaining business continuity.

Recover – Organizations need to adjust their cyber incident response processes and playbooks to prepare for a destructive malware scenario where there is the potential of catastrophic business impact. Organizations need to update mitigation strategies and align multiple parts of the organization including the executive team, communications teams, customer-facing departments and business partners.

An executive summary is available upon request. A more detailed paper for financial institutions is available within the FS-ISAC portal and on the Financial Services Sector Coordinating Council website. This detailed paper may also be useful for non-financial institutions that are deemed to be part of the nation's "critical infrastructure."

About FS-ISAC

The Financial Services Information Sharing and Analysis Center (FS-ISAC) is a non-profit corporation that was established in 1999 and is funded by its member firms. The FS-ISAC is a member-driven organization whose mission is to help assure the resilience and continuity of the global financial services infrastructure and individual firms against acts that could significantly

impact the sector's ability to provide services critical to the orderly function of the global economy. The FS-ISAC shares threat and vulnerability information, conducts coordinated contingency planning exercises, manages rapid response communications for both cyber and physical events, conducts education and training programs, and fosters collaborations with and among other key sectors and government agencies.

# # #