Testimony of John W. Carlson on behalf of the

The Financial Services Information Sharing & Analysis Center (FS-ISAC)

Before the U.S. House of Representatives Committee on Financial Services

June 24, 2015

Chairman Fitzpatrick, Vice Chairman Pittenger, Ranking Member Lynch, and members of the Task Force to Investigate Terrorism Financing, thank you for inviting me to testify at this hearing, "Evaluating the Security of the U.S. Financial Sector." My name is John Carlson, and I am the Chief of Staff of the Financial Services Information Sharing and Analysis Center (FS-ISAC). I am testifying on behalf of Bill Nelson, President and CEO of the FS-ISAC, my FS-ISAC colleagues and our membership.

You asked me to discuss "the security of the U.S. financial sector." My testimony provides: a) an overview of the FS-ISAC, including our role in information sharing and collaboration; b) an overview of the security threats facing financial institutions; an overview of key regulatory requirements and the strong risk management culture in the financial services sector; and c) suggestions for actions the Congress could take to improve information sharing and enhance the security of the U.S. financial sector.

FS-ISAC BACKGROUND

The FS-ISAC was formed in 1999 in response to Presidential Decision Directive 63 (PDD 63) of 1998, which called for the public and private sectors to work together to address cyber threats to the nation's critical infrastructures. After the 9/11/2001 attacks and in response to

Homeland Security Presidential Directive 7 (and its 2013 successor, Presidential Policy Directive 21) and the Homeland Security Act, the FS-ISAC expanded its role to encompass physical threats to the sector. The FS-ISAC is a 501(c)6 nonprofit organization and is funded entirely by its member firms and sponsors.

The FS-ISAC's 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's goals are to disseminate and foster the sharing of relevant and actionable information and analysis among participants to ensure the continued public confidence in the global financial services and to protect the financial services sector against cyber and physical threats, vulnerabilities, and risk. We act as a trusted third party that facilitates sharing of actionable threat, vulnerability and incident information (both attributed and non-attributed) and trusted manner among members, the sector, and its industry and government partners, ultimately benefiting the nation.

The FS-ISAC has grown rapidly in recent years. In 2004, there were only 68 members which were mostly large financial services firms. Today, we have about 6,000 member organizations, including commercial banks and credit unions of all sizes, markets and equities firms, brokerage firms, insurance companies, payments processors, and 40 trade associations representing all of the U.S. financial services sector. Because today's cyber criminal activities transcend country borders, the FS-ISAC has expanded globally and has active members in over 35 countries.

Since its founding, the FS-ISAC's operations and culture of trusted collaboration have evolved into a successful model for how other industry sectors are organizing themselves around this security imperative. FS-ISAC information sharing activities include:

- Delivery of timely, relevant and actionable cyber and physical email alerts from various sources distributed through the FS-ISAC Security Operations Center (SOC);
    - The appendix includes samples of our communications to members that convey, among other things, the type of alert, criticality level, and how the information should be handled, leveraging our "traffic light protocol"(TLP).
- An anonymous online submission capability to facilitate member sharing of threat, vulnerability, incident information and best practices in a non-attributable and trusted manner;
- Support for attributable threat information exchange by various communities of interest and circles of trust representing chief information security officers and business continuity executives, payments processors, and clearing houses.
- Regular threat information sharing calls for members and invited security/risk experts to discuss the latest threats, vulnerabilities, and incidents affecting critical sectors;
- Rapid response briefings to members when a broad-scale threat or attack is imminent or underway;
- Emergency threat or incident notifications to all members using the Critical Infrastructure Notification System (CINS); and

- Participation in various cyber exercises such as those conducted by DHS (Cyber Storm I, II, and III) and support for cybersecurity exercises such as the Hamilton series, CyberFIRE, and Quantum Dawn as well as member-led exercises such as the Cyber Attack against Payment Processes (CAPP) simulation exercises that the FS-ISAC sponsors.

Working with our members and other organizations, the FS-ISAC is engaged in numerous initiatives to:

- Improve information sharing content and procedures between government and the sector;
- Help automate, distill, prioritize and make cyber threat intelligence actionable for our members;
- Conduct joint exercises to test our communications, response and resiliency protocols during incident scenarios affecting different segments of the financial system;
- Maintain an "All Hazards Crisis Response Playbook" and within it a "Cyber Response Coordination Guide" that leads incident responders and executive decision makers through decision and action processes based on identified impacts and severity of incidents;
- Develop industry best practices and resources that can be used effectively by smaller financial firms with limited cyber capabilities;

- Engage with other critical sectors (e.g., communications, energy, information technology) and international partners to understand and leverage our interdependencies;
- Encourage broader use of the voluntary National Institute of Standards and Technology (NIST) Cybersecurity Framework, including among small and mid-sized financial institutions across the country; and
- Develop best practices guidance for operational risk issues involving third party risk, supply chain, and cyber insurance strategies.

FINANCIAL SECTOR PARTNERSHIPS

In addition to supporting individual financial institutions, the FS-ISAC works closely with the Financial Services Sector Coordinating Council (FSSCC) and with numerous national and state-based financial associations, including the American Bankers Association (ABA), BITS/Financial Services Roundtable, Credit Union National Association (CUNA), Independent Community Bankers Association (ICBA), Securities Industry & Financial Markets Association (SIFMA), and state banking associations.

The FS-ISAC collaborates with other sectors, including energy/electric, telecommunications, merchants/retailers, real estate and others. The FS-ISAC coordinates with other information sharing organizations and currently serves as the chair of the National Council of ISACs (NCI). The FS-ISAC coordinates and collaborates with numerous government agencies, including: the U.S. Department of Treasury, U.S. Department of Homeland Security (DHS), regulatory agencies that are part of the Federal Financial Institutions Examination Council (FFIEC), U.S.

Secret Service (USSS), Federal Bureau of Investigation (FBI), the intelligence community, and state and local governments.

As one example of our partnerships, we announced in early May a strategic agreement with the newly created Retail Cyber Information Sharing Center (R-CISC). Through the agreement, FS-ISAC is providing key advisory services and best practices, operational support and technology capabilities to help R-CISC deliver on its core mission to provide threat information sharing and cyber security for retailers.

In addition, the FS-ISAC worked with R-CISC and the U.S. Secret Service in November 2014, on a joint advisory on "protecting merchant point of sale systems during the holiday season." The advisory recommended possible mitigations for common cyber exploitation tactics, techniques and procedures (TTPs) based on previous attacks. The FS-ISAC continues to work with U.S. Secret Service and the R-CISC and is currently working on a new advisory on securing merchant payment terminals and remote access.

Last week, we released a joint advisory with the FBI and USSS on a type of wire transfer fraud called "business email compromise". "Business e-mail compromise" involves the compromise of legitimate business e-mail accounts for the purpose of conducting an unauthorized wire transfer. After a business e-mail account is compromised (often times a Chief Executive Officer or Chief Financial Officer), fraudsters use the compromised account or a spoofed account to send wire transfer instructions. The funds are primarily sent to Asia, but funds have also been sent to other countries all over the world.

The FS-ISAC participates in a variety of information sharing and other strategic programs, including the following:

- The FS-ISAC embedded a representative on DHS' National Cybersecurity and Communications Integration Center (NCCIC) watch floor two years ago. FS-ISAC representatives, cleared at the Top Secret / Sensitive Compartmented Information (TS/SCI) level, attend the daily briefs and other NCCIC meetings to share information on threats, vulnerabilities, incidents, and potential or known impacts to the financial services sector. Our presence on the NCCIC floor has enhanced situational awareness and information sharing between the financial services sector and the government, as well as other critical sectors.

- FS-ISAC representatives sit on the Cyber Unified Coordination Group (Cyber UCG), and the group has been actively engaged in incident response. The Cyber UCG's handling and communications with various sectors following the distributed denial of service (DDOS) attacks on the financial sector in late 2012 and early 2013 is one example of how this group is effective in facilitating relevant and actionable information sharing.

- The FS-ISAC, in conjunction with partner association and government agencies, has been involved in planning and executing a series of sector-wide cyber exercises that test our ability to share information and respond to critical incidents collaboratively with our government partners. In response to some of the conclusions from recent exercises, the FS-ISAC has launched a task force with over 80 representatives from the financial

services sector and numerous government agencies to develop best practices on how to mitigate and respond to a potential destructive malware attack.

- Finally, the FS-ISAC and Financial Services Sector Coordinating Council (FSSCC) have worked closely with government agencies to obtain security clearances for key financial services sector personnel. These clearances have been used to brief the sector on new information security threats and have provided valuable information for the sector to implement effective risk controls to combat these threats.

SECURITY AUTOMATION: SOLTRA EDGE

In recognition of the need to speed the flow of threat intelligence, the FS-ISAC established a joint venture with the Depository Trust and Clearing Corporation (DTCC) in 2014 to develop an automated cyber threat information sharing capability known as "Soltra Edge." Soltra Edge decreases the time to decision and mitigation from weeks and days to hours and minutes by leveraging two standards that the Department of Homeland Security funded and the MITRE Corporation developed: Structured Threat Information eXpression (STIX™) and Trusted Automated eXchange of Indicator Information (TAXII™). Soltra Edge takes threat intelligence from a variety of sources, normalizes it, and prioritizes this data at network speeds, turning it into instant actionable intelligence. Since its launch in December 2014, Soltra Edge has been downloaded by thousands of organizations both within financial services and other sectors. Created by users for users, Soltra Edge is designed to dramatically reduce the time it takes for security analysts to process threat information.

Soltra Edge is voluntarily funded by contributions from 16 financial services companies. In fact, the support for funding Soltra Edge came directly with several CEOs of our member

companies who recognized the strategic importance of developing this capability more rapidly and encouraged others in the financial sector to provide funding.

THREAT ENVIRONMENT

The current cyber threat environment continues to evolve and intensify. Each day, cyber risk grows as attacks increase in number, pace, and complexity. Our members constantly adapt to this changing threat environment. We are no longer in the days wherein the threat was confined to individual hacktivists and fraudsters. We are now in an era of attacks by not only organized crime syndicates, but also nation-states and entities affiliated with terrorist operations. Correspondingly, the attacks have grown beyond webpage vandalism and fraud into large-scale, prolonged campaigns that threaten the availability of services to citizens and threaten the privacy and accuracy of their information.

Our sector is increasingly concerned with these threats, particularly with the potential for attacks that could undermine the integrity of the financial system through data manipulation or destruction. This growing threat affects all institutions in our sector regardless of size or type of financial institution (e.g., banks, credit unions, insurers, payment processes and brokerage, investment firms). Increasingly, and as we have recently witnessed, other sectors face these same threats.

Malicious cyber actors with increasing sophistication and persistence continue to target the financial services sector. These actors vary considerably in terms of motivation and capability,

from nation states conducting corporate espionage, to advanced cyber criminals seeking to steal money, to hacktivists intent on making political statements. Many cybersecurity incidents, regardless of their original motive, have the potential to disrupt critical systems.

There are numerous tactics that malicious cyber actors use to target institutions. Among these the following are concerning:

- Targeted spear-phishing campaigns. These fraudulent emails, which appear to be legitimate, trick users into supplying sensitive information such as passwords that can result of the theft of online credentials and fraudulent transactions.
- Ransomware attacks in which malware is downloaded that restricts access to an infected computer (often via encryption) until a ransom is paid (often in Bitcoin).
- Distributed denial of service (DDoS) attacks which can impede access to services for extended periods of time.
- Business email compromise which involves the compromise of legitimate business e-mail accounts for the purpose of conducting an unauthorized wire transfer. After a business e-mail account is compromised (often times a CEO or CFO), fraudsters use the compromised account or a spoofed account to send wire transfer instructions.
- Supply chain threats.
- Blended physical and cyber attacks. An example of this is the theft of card data that is then used to steal money from ATMs around the globe using individuals who serve as "money mules".
- Insider threats.

The quote often attributed to Willie Sutton that he robbed banks "because that's where the money is" reminds us as to why financial institutions are often the subject of cyber-attacks. However, that quaint quote does not capture the entirety of the situation we face today. We also are observing that financial institutions are being targeted in response to international conflicts.

Perhaps the best visible example of this was the distributed denial of service attacks in 2012 through 2013 when an organization backed by a foreign country targeted dozens of financial institutions. The attacks were disruptive but they also resulted in unprecedented levels of information sharing among financial institutions and the US government. Information sharing proved to be extremely beneficial to firms that were targeted on the second, third and fourth wave of DDoS attacks given that the lessons learned from firms on the first wave were rapidly shared with others that had yet to be attacked. The DDoS attacks also led to increased collaboration with the major Internet Service Providers (ISPs) with financial institutions, facilitated by the FS-ISAC and BITS/Financial Services Roundtable.

The DDOS attack also catapulted the cybersecurity issue to a CEO level across the entire financial services sector for the first time. When the CEOs of our member financial services companies engaged directly it resulted in even greater collaboration among the financial associations and government agencies.

Being a focus of the attacks is certainly one reason why the financial sector has historically led the way in making huge investments in not only security infrastructure and the best-qualified

people to maintain the systems, but also in driving collaboration across industries and with the government. The primary reason for these investments is the recognition that customers trust financial institutions to protect them – to protect their investments, their records and their information. Individual financial institutions invest in personnel, infrastructure, services, and top-of-the-line security protocols to protect their customers and themselves and to respond to cyber-attacks. These investments protect the individual institutions and their customers, but on its own, an individual institution generally only has the ability to protect what is within its control. However, financial institutions are interconnected to others in the sector, with other sectors, and with the government. This reliance on others gives us in the financial services sector a unique and critical role in the cyber landscape and requires coordinated action for the most effective response. Recognizing the cyber threat environment continues to expand in complexity and frequency and that individual institution efforts alone will not be enough, executives from the financial services sector have stepped up efforts to work together.

RISK MANAGEMENT CULTURE, COLLABORATION AND REGULATION

In response to the changing threats, the FS-ISAC is working closely on risk mitigation strategies with numerous government agencies, including the U.S. Treasury Department, financial regulators, the Department of Homeland Security, and law enforcement agencies. These efforts build on the strong risk management culture within the financial services sector, in conjunction with extensive regulatory requirements.

Accordingly, we are striving to:

- Implement and maintain structured routines for sharing timely and actionable information related to cyber and physical threats and vulnerabilities among firms, across segments of the financial industry, and between the private sector and government and increasingly, to help properly share information between sectors.
- Improve risk management capabilities and the security posture of firms across the financial sector and the service providers they rely on by encouraging the development and use of common approaches and best practices.
- Collaborate with government agencies, other industry sectors, and international partners to respond to and recover from significant incidents.
- Discuss policy and regulatory initiatives that advance infrastructure resiliency and security priorities through robust coordination between government and industry.

We have learned that a strong risk management strategy for cyber and physical protection involves creating communities of trust in which professionals appropriately share information about threats, vulnerabilities, and incidents affecting those communities. That strategy is based on the simple concepts of strength in numbers, the neighborhood watch, and shared situational awareness. Sharing this information helps to prevent incidents from occurring and to reduce the risk of a successful incident at one firm later impacting another. These efforts increasingly focus on including smaller firms and international partners into the trusted community.

The financial sector is correctly credited with having a robust cyber security risk management culture. This is due, in part, to the fact that financial services are heavily regulated, and also to

the overarching imperative that our business models, consumer confidence, and the stability of the financial system and the global economy are dependent upon a secure and resilient infrastructure.

I certainly don't want to leave you with the impression that the financial sector needs more regulation to address the security challenge. Title V of the Gramm-Leach-Bliley Act of 1999 (GLBA) directed regulators to establish standards for financial institutions to protect customer information. Pursuant to GLBA, regulators have imposed broad information security requirements for regulated financial institutions with strong enforcement authority. In addition to issuing regulations over a decade ago, the federal financial regulators have issued extensive "supervisory guidance" that outlines the expectations and requirements for all aspects of information security and technology risk issues, including authentication, business continuity planning, payments, and vendor management." Regulators, for example, have imposed detailed requirements mandating strong internal procedures, vigorous threat and risk assessments, ongoing testing and evaluation of security systems, and required reporting to senior management and directors. Among the obligations to secure systems and protect data under GLBA and supervisory guidance, financial institutions must:

- Develop and maintain an effective information security program tailored to the complexity of its operations;
- Conduct thorough assessments of the security risks to customer information systems.
- Oversee service providers with access to customer information, including requiring service providers to protect the security and confidentiality of information;

- Train staff to prepare and implement information security programs;
- Test key controls, systems, and procedures and adjust key controls and security programs to reflect results of such ongoing risk assessments;
- Safeguard the proper disposal of customer information; and
- Update systems and procedures taking into account, for example, technology changes, emerging internal or external threats to information, changing business arrangements (e.g., mergers and acquisitions), personnel changes, and more.

It is also important to remind the Committee that financial institutions must comply with cybersecurity requirements and guidance from numerous regulatory bodies depending on their charter and activities. These regulatory bodies include the Commodity Futures Trading Commission, (CFTC), Consumer Financial Protection Bureau (CFPB), Federal Deposit Insurance Corporation (FDIC), Federal Reserve Board (Fed), Financial Industry Regulatory Authority (FINRA), Office of the Comptroller of the Currency (OCC), Securities and Exchange Commission (SEC), and numerous state banking agencies.

While regulatory requirements are a powerful and effective way to ensure that financial institutions have adequate controls in place, a growing challenge facing financial institutions today is the need for greater coordination and harmonization among the regulatory agencies, within the US and globally, to keep pace with new threats, new financial business process models, and the necessary skill sets to evaluate the intersection of those two for security and resiliency purposes. A common refrain we hear from senior executives and practitioners alike is

the need for regulators to harmonize regulatory requirements at both the policy and examination levels in order to reduce unnecessary regulatory compliance burdens and to better focus limited resources to mitigate cyber risks. While there are important efforts to coordinate among the independent regulatory agencies, more can and should be done to enhance regulatory coordination so that financial institutions are properly focused on enhancing security and resiliency and minimizing unnecessary regulatory burden.

It is also worth noting that financial institutions that handle payment information are also required to comply with non-regulatory standards, such as the Payment Card Industry Data Security Standard (PCI DSS). This also adds to the compliance burden to financial institutions as well as merchants and other organizations that handle payment information.

While not a regulatory requirement, regulatory agencies are reviewing the National Institute of Standards and Technology (NIST) Cybersecurity Framework to determine whether and how to harmonize and align regulatory requirements. The NIST Cybersecurity Framework was released in February 2014 in response to Executive Order 13636 of 2013 "Improving Critical Infrastructure Cybersecurity." The executive order directed NIST to seek private sector input through a collaborative process in developing a voluntary cybersecurity framework for critical infrastructure sector.

The Framework is a good example of public-private sector collaboration. NIST's successful approach at inclusion of so many essential parties reflects how broadly the Framework has been embraced by so many sectors. It synthesizes a process for cyber risk management that is

accessible from the boardroom to the operations floor, across not only individual enterprises but also entire sectors. It is a "Rosetta Stone" in that it provides a common lexicon for categorizing and managing cyber risks across sectors and enterprises for various unifying risk management jargons and creates a common understanding around various risk management terms, methodologies, ideas and language. It relies on international standards and is consistent with the regulatory requirements that have been in place for our sector for more than a decade. Down the road, the Framework has the potential to act as a baseline standard for cyber-insurance underwriters which could benefit multiple sectors by encouraging more secure and resilient cyber controls.

HOW CONGRESS CAN HELP

While the FS-ISAC and other information sharing organizations can provide many legal protections through member agreements, procedures and technologies, effective cyber threat information sharing legislation would enhance these capabilities to better match the increasing cyber threats that the public and private sectors face by providing targeted liability and disclosure protections. Effective cyber threat information sharing legislation includes the following elements:

- Facilitate real-time sharing to enable institutions and government to act quickly.
- Provide a targeted level of liability (such as a "good faith defense") and disclosure protections for cyber threat information sharing and receiving between individual institutions, through existing sharing mechanisms (such as the FS-ISAC), private to government, and government to private mechanisms.

- Provide protection from disclosure requirements through the Freedom of Information Act (FOIA), state sunshine laws, and to prudential regulators.

- Facilitate the appropriate declassification of information by the intelligence agencies and expedites the issuance of clearances to appropriate private sector individuals.

Bear in mind that the cyber threat information that the financial industry and lawmakers are talking about sharing are threat indicators that describe the type of malicious code sent to financial institutions, the route that malware took, and the means to protect it. This idea is very similar to law enforcement officials sharing data about physical crimes with the public and media outlets when a crime occurs or is attempted.

- What did the perpetrator look like?
- What kind of weapon was used?
- What did the getaway vehicle look like?
- Where did the criminals come from?
- Where did they go?

It is this type of information that, when shared, can be used to solve a crime or, perhaps more importantly, prevent more crime.

The Congress could also help by encouraging regulators to harmonize cyber security regulatory requirements.

In addition, the Congress could encourage the Administration to:

- Facilitate the appropriate declassification of information by the intelligence agencies;

- Expedite the issuance of clearances to appropriate private sector individuals;
- Recognize ISACs and the special operational role that they play in critical infrastructure protection and resilience and encourage owners and operators of critical infrastructure to join their respective sector ISACs;
- Support private sector efforts to form Information Sharing and Analysis Organizations (ISAOs) in the very few critical infrastructure sectors where they do not currently exist;
- Encourage all of the ISACs be represented on the NCCIC floor; and
- Recognize the National Council of ISACs as the coordinating body for the ISACs

CONCLUSION

Each week, more businesses, government agencies, and customers are victims of cyber attacks. The private sector is obviously waging a battle against adversaries whether they are launched by organized crime, organizations supported by other nations, or hacktivists. The FS-ISAC is responding by expanding our capabilities to share information in an automated way and to build stronger partnerships within the financial sector, with other sectors, with government agencies and with global partners. While the financial sector is an example of strong and frequent cyber collaboration and investment, we cannot fight this battle alone. Congress and the Administration can play a constructive role by enacting cyber threat information sharing legislation, encourage financial regulators to harmonize regulatory requirements, and support other efforts to enhance information sharing and cyber protections.

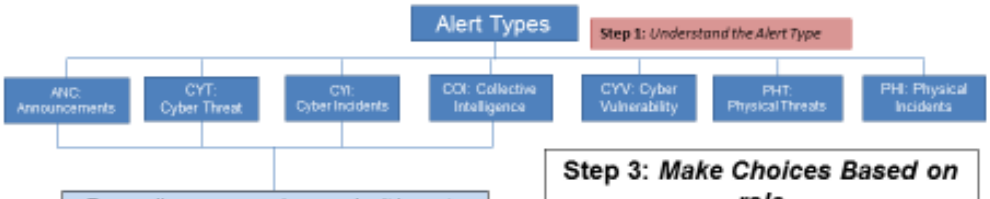
Appendix: Understanding FS-ISAC Communications

Understanding FS-ISAC Emails and Alerts

Determining which information is of value to your organization is one FS-ISAC cannot know. We can however, assist in providing you with guidance in parsing and forwarding FS-ISAC Alerts.

The email "subject" line in FS-ISAC alerts sent to the membership uses the following format

- ***[Alert_Type][Criticality]: [Alert_Title]***



Depending on your role, you don't have to follow every update, but FS-ISAC recommends following these key reports. Doing so will limit emails to about 10/day

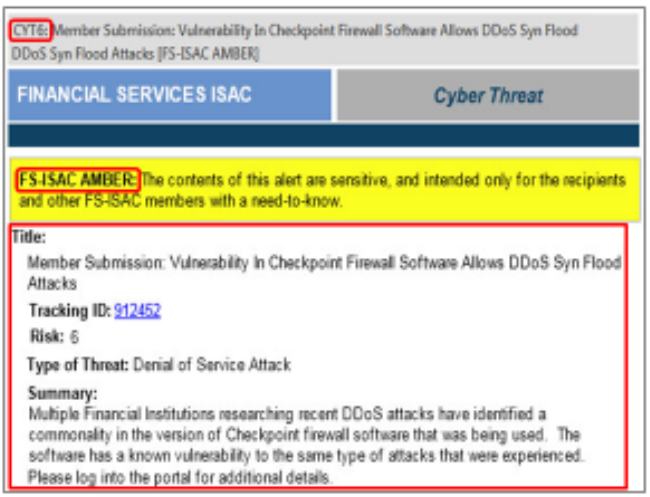
Step 2: *Understand the Criticality and Priority*

- ANC = Priority – 1-10, 8-10 is high priority
- CYV = Risk – 1-10, 8-9 is Urgent, 10 is Crisis
- CYT = Risk – 1-10, 8-9 is Urgent, 10 is Crisis
- COI – No Criticality Metric
- PHT = Risk – 1-10. 8-9 is Urgent, 10 is Crisis

Step 3: *Make Choices Based on role*

- Analysts and those involved in risk assessment or vulnerability/patch management should receive CYV alerts.
- Intelligence analysts may also want to participate on the Cyber Intel listserv. POCs are automatically added, but a portal account is not necessary if you wish to add additional analysts to the distribution
- Provide portal accounts to your staff based on each individual's role. This will allow them to employ portal filtering for their unique assignments
- We provide summary reports for mangers and technical reports for analysts. Making informed choices based on your role eliminates unneeded emails

Key Components of Alerts



The abbreviation and criticality level will always appear in the subject line, along with the title

Be aware of FS-ISAC's Traffic Light Protocol

Following the TLP Color, the alert will go into more detail such as the type of threat, summary, and handling instructions