Ken Leonard: ITS standards can make your life easier. Your procurements will go more smoothly and you'll encourage competition, but only if you know how to write them into your specifications and test them. This module is one in a series that covers practical applications for acquiring and testing standards-based ITS systems.

I am Ken Leonard, director of the ITS Joint Program Office for USDOT and I want to welcome you to our newly redesigned ITS standards training program of which this module is a part. We are pleased to be working with our partner, the Institute of Transportation Engineers, to deliver this new approach to training that combines web-based modules with instructor interaction to bring the latest in ITS learning to busy professionals like yourself.

This combined approach allows interested professionals to schedule training at your convenience, without the need to travel. After you complete this training, we hope that you will tell colleagues and customers about the latest ITS standards and encourage them to take advantage of the archived version of the webinars.

ITS Standards training is one of the first offerings of our updated Professional Capacity Training Program. Through the PCB program we prepare professionals to adopt proven and emerging ITS technologies that will make surface transportation safer, smarter and greener which improves livability for us all. You can find information on additional modules and training programs on our web site www.pcb.its.dot.gov

Please help us make even more improvements to our training modules through the evaluation process. We look forward to hearing your comments. Thank you again for participating and we hope you find this module helpful.

Nicola Tavares: Hello. Welcome to Module CSE202: Introduction to Cybersecurity for Transportation Agencies. Your instructors today are Ralph Boaz is a transportation industry expert in the advancement and use of intelligent transportation systems, ITS. Through technology and standardization, Mr. Boaz assists agencies and private companies in the planning, specification, deployment and testing of ITS equipments and systems. Prior to starting Pillar Consulting, Mr. Boaz was a computer scientist working in artificial intelligence and parallel processing and later he was Vice President of Engineering for Econolight. He was a subject matter expert for the Roadway Transportation System Cybersecurity Framework Project and is currently working on cybersecurity projects for the USDOT.

We also have Mr. Eisenhart who has 45 years of experience in system engineering including 26 years in ITS. He has been involved in all phases of system development and operational concepts and requirements definitions through design to system testing. He is one of the foremost experts on the subjects of ITS architecture development. He was a system engineer for the FHWA project to develop the roadway transportation systems cybersecurity framework. I now turn this presentation over to your instructors.

Ralph Boaz: Hello, I am Ralph Boaz and on behalf of Bruce Eisenhart and myself we would like to thank you for participating in Professional Capacity Building (PCB) program and particularly this module. These are our learning objectives today. We will, Bruce and I, will alternate going through each of the objectives and hopefully we'll keep you engaged and you'll enjoy the course.

Our first learning objective is recognizing the need for cybersecurity and if you're here you probably already know that you need cybersecurity to some degree. And under this learning objective we will add some depth and share some vulnerabilities and threats. Secondly, we'll describe the NIST cybersecurity framework, and NIST stands for the National Institute of Standards and Technology and it provides guidelines for how organizations can assess and improve the ability to secure environments, manage risks, and respond to threats. Thirdly, we'll tie the cybersecurity framework to your organization helping you to establish and improve your cybersecurity program. And then fourth learning objective is to identify resources for information sharing and that's where you can find information, talk about what to report and where to report incidents.

Learning objective 1 is recognizing the need for cybersecurity. In this learning objective we'll talk about terminology. We'll talk about critical infrastructure and discuss the traffic operations environment. We'll talk about the different types of attacks and threats. We'll talk about areas of vulnerability in traffic operations and we'll share some interesting cyberattacks.

Now for consistency in this module, most of our definitions are going to come from the NIST cybersecurity framework or from the NIST glossary of key information security terms. The glossary identifies the sources for the definitions as well, so it can be a pointer to other sources. So let's define cybersecurity or sorry, cyberspace, and that's the independent network of information technology infrastructure, so that includes internet, telecommunications, networks, computer systems and embedded processors and controllers in our industry.

So what's a cyber-attack? That's an attack via cyberspace that targets our organization's use of cyberspace for the purpose of disrupting, disabling, destroying or controlling our computer environments or infrastructure. It can also be the destroying of the integrity of data or stealing controlled information.

Cybersecurity, that's the process of protecting the information through preventative, through detection and the response to attacks. And that's also said to be the ability to protect or defend the use of cyberspace from cyberattacks.

Resilience, this is the ability to operate under adverse conditions and it's also said to recover to an effective operational posture. It's the ability to quickly adapt and recovery from any known or unknown changes in the environment. So this is a great word and this would be a great thing to say about your organization, that it's resilient.

Attack vector, this is a techie term it sounds like, and it's a path or means by which an attacker can gain unauthorized access to your computer systems. There's lots of well-known examples of that. Email attachments, pop-up windows, chatrooms, viruses, text messages. One that's not on this list might be something as simple as a bad actor dropping a USB drive right outside an office door and somebody picks it up and then plugs it into their computer and they now have some sort of malware or something on their system. Those are just examples of the way in.

So there has been an organization formed called CISA, Cybersecurity and Infrastructure Security Agency, and it's under the oversight of the Department of Homeland Security and it has identified 16 critical infrastructures for the United States. They're all listed here and they are

described in the Student Supplement. And we're going to be talking about the Transportation Systems Sector.

Within the Transportation Systems Sectors you see it has different sections. Aviation, highway and motor carrier, maritime transportation and others. Oh, you see freight rail down there and postal and shipping. Those are all covered under Transportation Systems Sector. We're going to be talking about the highway and motor carrier area.

So the concerns of this part of the sector is over 4 million miles of interstate highways and roads; over 614,000 bridges; 519 tunnels; trucks; commercial vehicles; vehicle and licensing systems; and the areas of our concern today will be traffic management systems and cyber systems for operational management. I want to make the point that under traffic management systems this includes approximately 350,000 signalized intersections.

So now we're going to talk about the scope of concern for traffic operations. Of course we have in our traffic management centers we have the computers and networks that are there and that's what this picture represents. So other concerns are the field equipment that is used to control traffic signal systems but also do things like street lights and dynamic message signs, maybe some parking access. We have video surveillance. There's lots of field devices out there that may be under the control or concern for traffic operations.

And then we have the communications which we call center-to-field communications between the central systems and the field devices. Then we also have external cloud computing which has come on strong in the last several years. And that is used quite a bit by traffic management centers but it's also now being used by some field devices to store data as well. So we have external cloud computing being part of the concern for traffic operations. Then we have systems that are outside of the particular traffic ops network which might be other agency systems within the organization like business systems, et cetera, or they can be non-agency systems like from another agency, for instance. Maybe there's a transit center that's outside of that that communicates with the traffic ops network, et cetera. So we call that center to center communications and there may be other types of communications used in these cases.

Then we also have which everyone's hearing about now is the connected vehicle world or connected V2X which means vehicle to everything technology. And we have wireless connections to those from the field to on board units on cars and mobile units carried by people that will be connected from the field equipment to those devices. And then we might have as shown here in the bottom right, we might have remote users connecting into the central systems and in this case remote user is someone who might be on their own personal computer. If someone was on a work computer that has a special connection into the traffic operations (ops) network, then that's covered already by the previous picture.

And then we might have a remote user again coming directly into field devices. And so we're concerned about that. Now let's draw a boundary here. So what's inside this boundary is the equipment and networks that the traffic operations people need to protect and need to be concerned about. The devices and systems that are outside the boundary are of concern to use from as far as the interfaces to them is concerned. So the traffic operations is concerned to the interfaces to these things outside the boundary but we're not concerned about the systems or devices themselves.

Okay in the next couple of slides, these are the words that summarize what we just went through pictorially and so you can look back at this as you go through this module or pause it to see, to review what I just said.

Again, these are the cybersecurity concerns outside of traffic ops control. The travelers and the modes of transportation are outside of our control. The systems of those used, the systems that are outside of those used in traffic ops, for instance the cloud computing, we're worried about the interface to cloud computing, we're not worried about cloud computing itself. Non-agency system, we're just worried about the interface. Cloud-based systems, we're just worried about the interface.

Okay, now we're going to talk about the sources of cyber-attacks and they are many. We'll just talk about a few of them here. We have criminal groups and those criminal groups seek to attack systems for monetary gain. Again, that's organized crime groups using spam, phishing, spyware, and malware. They want to commit identity theft and online fraud. We have foreign intelligence services. They use cyber tools as part of their information gathering and espionage activities. There are several nations out there that are aggressively working to develop information warfare doctrine programs and capabilities as example, and such capabilities enable a single entity to have significant serious impact by disrupting the supply communications and economic infrastructures that support military power. And we have hackers, which is, you know, everywhere. And in fact, you know, in some cases hackers are doing things for bragging rights while in other ways they're looking for money, etc. But we have there's a lot of tools that have been developed and that are more sophisticated and also easier to use.

So, there is a growing number of hackers but most of the hackers and a smaller percentage of them would have the capabilities to target a major critical infrastructure but they are out there. And probably on this list that is a principle source of computer crime is the disgruntled organization insider and because they may not—they may have a great deal of knowledge about the computer systems they're using. They know how to get in. They may have unrestricted access to cause damage or to steal important data.

So, we'll talk about several types of attacks and threats. There's a denial of service (DoS) attack and that's when a computer or computer system is it becomes a target of a bunch of noise or like log ins and things like that to the point that there's so much information and messaging and such flying towards that system that it becomes unusable to the people who need it. Now a DDoS, a Distributed Denial Of Service attack, that's where you have many computers doing the same thing and that's on a major scale that's how they really tie up your computer system or your device.

Then we have malware attacks. That's hardware, firmware, or software that's intentionally included or inserted in the system for harmful purposes. And ransomware is where they do that to get money back from the target's operator. And we'll talk about a ransomware attack a little later in this presentation. And you have a password attack. That's sometimes called password cracking. And there's various ways they do this. They can do a brute force attack, which they just repeatedly try to guess what the password is. And this could happen over a long period of time.

There's also a dictionary attack where they have a set of stored commonly used passwords. It could be a big list but they use that and then there's other cryptographic methods that they do that, that they'd use to break into systems. And then we have eavesdropping. That's an attack where the attacker listens passively to the authentication protocol to capture information that can be used on subsequent attacks. They can again sit there and eavesdrop for a long period of time until they get the information they need and/or credit card numbers or other confidential information they may want to use to exploit.

Okay, the types of hackers. We have black hat, gray hat and white hat hackers. This is a simple view. There's probably something along the lines of, you know, 10 or so or more different types of hackers that some organizations may call out. But this is a simple view. Black hat, gray hat and white hat. Black hat comes from the old Westerns that always had the bad guy in the black hat. And the black hat hacker is an individual who attempts to gain unauthorized entry into a system or network and to exploit it for malicious reasons. A white hat hacker is of course the good guys and they are there to strengthen the security of the organization. A white hat hacker has permission to engage the targets and to compromise them within prescribed rules of engagement. And then we have the gray hat in the middle.

And as you might expect, it is kind of in the middle position. Gray hat exploits the networks and computer systems in the way that the black hats do, but they do it without malicious intent and there is an element of pride here, but they disclose loopholes and vulnerabilities to law enforcement agencies or to the companies themselves. However, there is also the hope of some financial compensation for doing such things. Like I said, in the Student Supplement there will be other types of hackers described there.

Okay, now we'll talk about the vulnerabilities to our traffic operations. There's a use of advanced computing and sensing and communications in our roadway systems that is important and we need those to meet operational needs, but that also increases cybersecurity risks.

Transportation controllers themselves, we have modern controllers that are Linux computers and they'll support multiple and concurrent on street applications so you have maybe a bigger effect from attacking them. And they also have the benefit and some vulnerabilities that a full-fledged computer has. But and then we also have, let's say we have controllers that are about 10-years old. In that environment they may not have critical operating system updates and software patches.

So, in modern computer systems we really need to be concerned about cybersecurity. Now the communications that we use in traffic operations, we need to be concerned about that because many of us came through when we used to have serial lines and it just generally was not accessible to outside the agency, but now we're using IP and Ethernet type of communications everywhere.

One of the concerns that we have right now is the primary protocol used for center to field communications is NTCIP, which is the National Transportation Communications for ITS Protocol, and that currently does not have security built into it. And generally, communications are not encrypted by other means. So we need to make NTCIP secure. Other, some more larger agencies are encrypting all their communications and so they are protecting it that way,

so external to the protocol itself. But we are actually currently on a project to help make NTCIP secure.

So one of the things that has occurred to us is a state-sponsored attack. This goes back to as we were talking about the espionage type of situation when we're talking about attackers. And state sponsored attack on our infrastructure could result in signal timing changes, blocked sensor calls and flash conditions. Now there is a signal monitor unit that's inside cabinet systems that protects the public from conflicting colors like an eastbound and a northbound green light. That does not happen like it does in the movies. There is a device in the cabinet that prohibits that from happening. But still, these signal timing changes, for instance, could create delay. Now what's the cost of delay? Well, that really affects large cities, large metropolitan areas and will affect the regions around them.

In 2009, there was a report that traffic delays in Los Angeles cost $12.8 billion dollars a year and that's approximately $1.46 million dollars per hour. So somebody, you know, some nation state that is antagonistic towards us can create quite a problem in a metropolitan area if they could just induce delay across the region and across the area. Of course we have physical vulnerabilities and many of you taking this course will be aware that the #2 key has been used in traffic control cabinets across the country for decades. That is actually being changed out. People are going to more sophisticated locks, push button locks and then some really sophisticated programmable locks are going on in cabinets today. But that's still a process of change. While the concerns is just the people element just like when attackers depend on, yeah, use phishing schemes to get people to buy in from inside the agency, we out in the field sometimes cabinets are left unlocked and that's where they've had people hack into dynamic message signs on the road because simply because the cabinet was unlocked and somebody got access to it. So infrastructure owner operators need to be concerned about cybersecurity in their design and operation of their systems. And it's not just an IT issue. It's an everybody in the organization type of issue. So far, all known hacking into traffic signal systems has been done in a white hat capacity, which is good.

Okay, now we have a couple little examples to share with you. Colorado DOT had a ransomware attack in 2018. It was called SamSam and the ransom amount wasn't published but there was 2,000 computers taken offline for several weeks to prevent further damage. The state formed a command group to implement a four-phase approach to solve the problem. There was $1.5 million dollars spent to undo the damage after they refused to pay the ransom. I need to make a point here, though, that this did attack the DOT but it was not in their signal systems, it was their business network only.

Okay, the Sacramento Regional Transit had an attack in 2017. The attack erased parts of their computer programs on the agency's servers and that affected the internal operations including the ability to use computers to dispatch employees and assign bus routes. Rail and bus services themselves did not get affected. So there was about 30 million of 100 million files were deleted; 2,000 computers were taken offline over several weeks. They threatened to do more unless approximately $8,000 dollars was paid. The State again formed a command group over several weeks. And in all it was about $1.5 million to undo the damage after they refused to pay and about 80 percent of the deleted files were recovered. So you can see this is expensive and a concern to us.

Now we have an activity. We have a little question and based on the information I just gave. Which of the following is a true statement? Answer choices are A, Modern transportation controllers are less sophisticated than other cyber devices and easier to protect; B, Cybersecurity is an IT responsibility only; C, Traffic ops needs to protect any external cloud-based systems used; D, Transportation infrastructure could be a target for State-sponsored cyberattacks. Please make your selection.

If you said D, you were correct. A State-sponsored cyberattack could have a high economic impact on a large metropolitan area due to the cost of delay. If you said A, that was incorrect and that's because modern transportation controllers are sophisticated and they're full-fledged Linux computers. If you said B, that was incorrect. Cybersecurity is not only an IT responsibility, it's a responsibility of everyone in the organization. And if you said C, that was incorrect because traffic ops needs to protect the interface to external cloud-based systems, not the cloud-based systems themselves. And so that might have been a little tricky for you, but hopefully you got this right. All right, now I'll pass this on to Bruce.

Bruce Eisenhart: Thank you very much, Ralph. So, how does a transportation agency address cybersecurity? Well, a good way is through the use of the NIST cybersecurity framework and starting in this learning objective we're going to look at the structure and the content of this framework.

The NIST cybersecurity framework was originally created by Executive Order as it's shown there in 2013 and then there was a Cybersecurity Enhancement Act of 2014 that was created to fund its update and maintenance. As part of the development of this framework, the framework is defined as a prioritized flexible repeatable performance-based and cost effective approach to manage cybersecurity risks for those processes, information and systems directly involved in delivery of critical infrastructure systems. It provides an approach to assess, identify, and manage cybersecurity risks for critical infrastructure systems and it provides guidance to organizations on how to plan for and deal with cybersecurity risk.

The framework was developed in conjunction or in collaboration with industry. It's a technology neutral framework that talks about what you do and the activities to do it. The current version of the framework is version 1.1 which came out in April 2018. The framework is composed of three parts. The first part is the core and that will be the subject of this learning objective and I'll expand directly on that. The second one tier stands for implementation tiers and these provide the context on how an organization views cybersecurity risks and the processes in place to manage that risk. And finally, profiles represent the outcomes based on business needs in an organization selected from the framework categories and subcategories that I'll mention soon. The profile can be characterized by aligning your standards, guidelines, and practices to the core in a particular implementation scenario. And the discussion of implementation tiers and profiles will be in the next learning objective, learning objective 3.

So, the framework core identifies cybersecurity activities and desired outcomes from those activities. It applies across all critical infrastructure sectors which include transportation and it is made up of five concurrent and continuous functions that I'm going to describe in more detail for the remainder of this learning objective.

Now the way the framework core is organized, there are the five functions and each function is broken into categories. The categories relate to needs and activities. Each category has a set of subcategories that are specific outcomes to those activities and for each subcategory is defined some informative references that provide section level references into six key technical cybersecurity documents. And as you can see from the table, the five functions have anywhere from 3 to 6 categories; 6 to 39 subcategories, and all but 1 of them includes a reference to each of those 6 informative references.

Now looking at categories, there are the subdivisions within each function. The first function, identify, has six categories and on this chart is listed the first which is, and I've got the exact words from the framework in here for that first category of asset management, and that says the data, personnel devices, systems and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

So that's an example of a category. And notice the IDs on each of the categories. So this is the ID function .AM for the asset management. So the framework has a sort of set of acronyms for each of the categories and subcategories that you can use to trace things.

Now a subcategory as I mentioned is list an outcome related to a category. And here is an example subcategory under asset management. This happens to be the first subcategory under asset management, so it's ID.AM-1. And the subcategory says physical devices and systems within the organization are inventoried. And then for each of these subcategories there are section level references for the 6 informative references. And then the first one here, the CIS critical security controls defines 20 controls that are best practices to mitigate the most common attacks against systems and networks.

This diagram on the bottom, which is a little hard to read, is a little piece of the framework that I've copied and put on here. The entire framework set of functions, core, rather, functions category, subcategories, and references is contained in the Student Supplement so you can see it there. And in terms of the informative references, for example, this AM-1, this is an informative reference, the first of the 20 controls which is defined in the CIS reference says, actively manage, inventory, track and correct all hardware devices on a network so that the only authorized devices are given access and unauthorized and unmanaged devices are found and prevented from gaining access. So that's an example of one of those CIS CSC controls.

Now I'm going to walk through each of the five functions of the framework core and I'm going to have two charts for each function. The first chart is going to give a definition of the function and then list the categories, and I'll briefly describe them. And then the second chart will talk to how this relates to the transportation critical infrastructure.

So the first one is identify. And identify means to develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data and capabilities. As you saw in the other chart, there are six categories. I already defined the asset management. Business environment is to understand the organization's mission, objectives, stakeholders, and activities. Governance is the policies, procedures and processes to manage and monitor the organization. Risk assessment seeks to understand cybersecurity risk to organizational operations, assets and individuals. The risk management strategy is the organization's priorities, constraints, risks,

tolerances and assumptions. And then the supply chain risk management are risk decisions associated with managing of the supply chain.

So this function addresses both information security and risk management. Under information security you define the processes that you need to manage your information. You also identify the roles and responsibilities. And finally, you're going to consider not just IT systems but also the operational systems, the centers, the field devices and the communications that goes between them. In the terms of risk management, the first thing is to perform a risk assessment and this is the assessment to the operations, operational organizational assets, organization supply chain and the individuals. Identify threats and vulnerabilities and these include threats and vulnerabilities to your field, center and communications network. And finally document these processes or strategies. So you have a documented set of risk management processes or strategies relevant to cybersecurity.

The protect function is to develop and implement appropriate safeguards to ensure delivery of critical services. This is one of the most important aspects of the framework from a transportation context. It involves developing and implementing the appropriate safeguards to protect all those assets, the centers, the field, devices and the communications. There are six categories. The first, identity management, authentication and access control looks at access of facilities and it looks at access as limited to authorized users, processes, and devices. In the area of data security, that information and records or data and databases, things like that, are managed to protect the confidentiality, integrity, and availability of the information. Information protection processes and procedures looks at the security processes and procedures that are used to manage the protection of your systems and the assets including the data. Maintenance looks at the maintenance and the policies you have for maintenance. Protective technology considers technical security solutions that are managed to ensure the security and resilience of your systems and assets. And then awareness and training is the idea of training people within your agencies to perform cybersecurity-related duties and responsibilities.

The protect function addresses device and system configuration management. This, you need to protect your devices, you need to have a good inventory of your systems and devices and in addition to having a good inventory you need to have a set of configuration change procedures so that you understand what changes are made.

Access control, the second one there, considers who can access the system and the devices and how they do so. Under data security, you need to consider both at risk data, meaning things you have in databases, and data in transit looking at the communications of data from field to centers or from centers to centers so you can protect the confidentiality, integrity and availability of agency information.

It also includes under data security integrity checking software, firmware, data in order to verify the agency's assets have not been compromised with virus or malware. Information protection procedures and processes, these include things like backup procedures and also procedures like data destruction procedures. How do you get rid of the data when they systems are taken offline?

Protective technology considers things like log records and audit records and you might under there have something like something called the principle of least functionality where you

configure systems to provide only needed capabilities and don't allow other capabilities to be accessed. And finally training, which provides cybersecurity and awareness training to personnel and to the partners you have, the vendors that may run and operate a lot of your systems.

The detect function looks to develop and implement appropriate activities to identify the occurrence of a cybersecurity event. It's important because detection is not always easy. Is it an attack or is it just a system malfunction? So, the categories under this are anomalies and events. Can you detect anomalous activity and what's the potential impact of the event and how do you understand the potential impact? Security, continuous monitoring. That your information systems and assets are monitored to identify cybersecurity events and to verify the effectiveness of the protective measures that you have defined. And finally, detection processes. How do you detect it's an event? What are your detection processes and procedures and how do you test that to make sure that they're working?

So the detect function addresses defining the system baseline. Establish a baseline of system and network operations, and we're going to be able to understand when a cyber event occurs. A baseline would need to consider the versions of hardware, software, firmware, configuration files and configuration records, system monitoring, monitoring the physical environment, central systems, the field devices, and the networks. Detecting malicious cyber events. As I said before, is it a cyber-attack or is it just a maintenance issue? And assessing events. Define the rules, practices, or principles that would help to assess whether something is a malfunction or a malicious cyber event.

The next function is the respond function to develop and implement appropriate activities to take action regarding the detected cybersecurity event. And there are five categories under this. The first is response planning. The response processes and procedures were executed to ensure response to a detected cybersecurity incident. Communications refers to response activities related to internal core communications and external communications.

Who do you call internally if there is an event and how do you respond to it and who do you call externally? Analysis is conducted to ensure effective response and to support recovery activities, analyzing to figure out exactly what happened. Mitigation activities are performed to provide—to prevent expansion of an event, to mitigate its effects and to resolve the incident if possible. And then, finally, improvements. Organizational response activities are improved by incorporating lessons learned.

This function addresses the idea that you need to devise and implement a response plan and the response plan needs to consider not just the incident response but also operations continuity, how you keep your operations up and running following an event. Assess the severity of attack, the scope of the event, and the impact of the event. What is its impact on operations? And then incident reporting. Internal, for example, the IT department might be the first people you call if you have something that affects operations. And external. You know, is there a triggering event? What would happen where you would bring in law enforcement or other organizations? And we'll actually talk in learning objective 4 about what are some of the other organizations you might be able to interface with to help as part of the response.

Recovery refers to the plan for and the implementing activities to restore the capabilities of services that were impaired due to a cybersecurity incident. How resilient are your operations? What's their ability to withstand and recover deliberate attacks? The three categories here are recovery planning. And so you have recovering processes and procedures that then you execute and they're maintained to ensure restoration of systems. Improvements, recovery planning, and processes are improved by incorporating your lessons learned. And then communications, again, both internal communications and external communications.

This final function addresses disaster recovery plans specific to a cyberattack, executing those plans following attack, how to get your systems back online. When the couple of examples Ralph gave, it took both of those groups something like four weeks to get their systems back online. And who do you communicate with, both internally and externally? So cyberattacks shut you down. What activities are required to get you online and who does them? What are the roles and responsibilities for those?

Now we'll do a short activity with a multiple choice question. The question is which of the following is not one of the NIST functions? Identify? Defend? Detect? Respond? Recover? The correct answer is defend. The actual framework function is protect, which covers a wider range of topics than the idea of just defending. And the others, identify, detect, respond, and recover are four of the other core functions of the NIST framework. With that, I'm going to turn it back over to Ralph to do learning objective 3.

Ralph Boaz: Thank you, Bruce. So as Bruce was going through learning objective 2, he was discussing the core functionality of the framework as it describes cybersecurity and he was going into the categories that were covered for each of the functional areas. Now each of those categories as he said also have subcategories and if you were to go to the framework and look at all the things that you could be doing about cybersecurity it can be overwhelming when you first see it. We don't want that to be an obstacle but just be thankful actually that somebody has, an organization has gone through and really thought through this and has identified different areas and so you can, so that other people that can use them in creating and maintaining their cybersecurity.

So, in this learning objective we're going to apply the cybersecurity framework to your organization and we're going to cover the framework implementation tiers and framework profiles. We'll talk about how to use those. And we'll do a basic review of cybersecurity practices, establish or talk about establishing or improving a cybersecurity program and self-assessing cybersecurity risks.

So framework implementation tiers. As Bruce said previously, the tiers provide a context of how an organization views cybersecurity risks and processes. And it's' really there to help us understand where we are at in the various categories and subcategories that are defined in the framework. There's four tiers: partial, risk-informed, repeatable, and adapted.

We don't want to confuse you. Again, I just want to emphasize that the tiers are there for to be able to measure where we're at. They describe the rigor and sophistication in cybersecurity risk management. There's three parts discussed for each tier. There's a risk management process. That's how well the practices work and how repeatable are they. We talk about integrated risk, the integrated risk management program. That's how well is risk management integrated into

the operation and decision making of the organization. And third, we talk about external participation. That's how well does the organization receive and incorporate cyber threat information from outside sources and also how well does the organization share cyber threat information that it generates with the other organizations?

I wanted to talk about, so here I'm going to go through each tier and talk briefly about the contents of that tier. I'm not going to hit on every aspect but I've highlighted some things to say here. So under risk management process in Tier 1: Partial, the practices are not formalized. There's some other ad hoc and sometimes reactive. If we're talking about the risk management program, there's a limited awareness of cybersecurity risk at the organization level and its implementation is irregular in case by case. And as far as external participation is concerned, the organization does not collaborate with or receive information from other entities. That's partial.

Tier 2 is Risk Informed. Regarding risk management process, the prioritization, this has to do with—well, sorry, the risk management process in the organization undergoes a prioritization of the cyber activities, which is good because that is a start. But the risk management practices are not organization-wide policy. So there's people in the organization doing this and there's priorities based on risk objectives and threat environment, et cetera. There's as far as the integrated risk management program is concerned there is an awareness of cybersecurity risks at the organizational level, but it's not considered at all levels of the organization. Under external participation, the organization collaborates and receives some information from other entities. So that's risk informed.

Tier 3 is Repeatable. Under risk management process, the practices are formally approved and expressed as policy. The practices are regularly updated. So this is becoming quite a, you know, a strong program here. As far as the integrated risk management program itself, there is an organization-wide approach to managing cyber risk. There's policies, process and procedures that are defined, implemented and reviewed and this is very important, from the top down, senior executives communicate regularly regarding cyber risk. That's repeatable. Oh, sorry, the external participation part of this, I'm sorry. The organization regularly receives information and may share on a different case-by-case basis internally generated information. So, that's repeatable.

So Tier 4 is Adaptive. Under the risk management process, we say it continuously improves cyber security technologies and practices adapting to the changing threat landscape. Under the risk management program, the organization manages cyber risk based on risk informed policies, process and procedures and they even go to the point of addressing potential cybersecurity events. Of course, the senior executives are very involved and then this is really important, the realization here is that the organizational budget is based on understanding of current and predicted risk environment and risk tolerance. Your budget to address this is a constraint and a lot of our organizations aren't set up to do that at this point.

So external participation, the organization collaborates with entities regularly receiving information, sharing it and sharing internally generated information. So, these are just ways for us to measure how we're doing within those categories and subcategories that are part of the core.

I want to talk about progressing. When you're thinking about selecting a tier for either where you're at or where you want to go, you want to base it on your business practices. Currently what are your security practices? What is the threat environment? Are there legal and regulatory things that need to be done? What are the business mission objectives of your organization? What are the agency constraints? So those all factor in when you're selecting the tier. When you're progressing on a tier, of course it's desirable to get better in any area but you're encouraged only to do it when there's a cost benefit analysis that says it's feasible and cost effective. So not only do we need all these things feeding into our decision making, we want to be smart about that from that perspective; we also need to be smart about, well, is this worth it at this point in time. So this is really helping us to create priorities, is what it's doing.

So, I want to emphasize that the tiers help us to support the decision making in regards to cybersecurity risks, but the tiers are not some sort of certification or something that is organization-wide. So, like, there is not a tier—we're a tier 2 company or a tier 3 company. It doesn't have anything to do with maturity. So, it's not maturity. It's not some sort of certification. This is strictly a tool.

So, we're going to illustrate this a little bit and hopefully this will help it sink in. So we have these functional areas that Bruce described and we have these categories and subcategories. That's what these columns represent or you could think of maybe each one of these columns would be in a subcategory, a category-subcategory combination there in the core. So, we have those. And then as we're trying to look at ourselves and look at where we want to go we have these tiers that help us define how well we're doing within those categories and subcategories. So the higher the tier, the more sophistication we have and rigor in our organization regarding the category.

So let's talk about Profiles. So profiles, that represents the outcomes that you're having based on the business needs selected from the framework functions, categories, and subcategories. So you may have, you know, a set of categories and subcategories that are important to your organization, so you want to capture all those and they're written out there for you in the core. And now you want to be able to see where you're at. So, we have what's called a current profile. The current profile that indicates the outcomes that you're currently having with your organization. And then you can have and you can do that across the board across the subcategories and categories.

And then you have a target profile. And that target profile indicates the outcomes needed to achieve your desired cybersecurity risk management goals. And you might do that on a yearly basis or it might have a five-year plan or things like that that it depends on your organization. And so we can compare the current profile and the target profile can help us to measure progress and make plans, etc.

So now I'm going to illustrate that a bit. So we have, so here's a situation where we have our framework down there and what we did was we analyzed our organization and we decided on these different categories and subcategories that this is where we were at. And we see that we still, that we have about six items that are down in the tier 1 area. So we capture that in a document or our current profile. And this is not like a checklist. There's no, like, spreadsheet to do this, at least that I know of, but this is a way I thought of representing what's going on during a self-assessment. Put that in the current profile.

Now we want to do one for the target profile so we discuss, we apply all our business needs and you know, all the things we talked about in tier progression, business needs, your current practices, regulatory things, all those things we talk about in tier progression. And we decide that well, we want to pull in identify, protect—identify, protect and respond, we want to move into tier 2 in the areas that we are addressing in our organization. So this shows what that might look like. And we have this restriction. We only have so much money or resources to use, so we're not going to be able to move recover, those items that are in recover at this point forward until at a later time. And so we put that in our target profile.

We can then do some planning in our organization on how to get there. And I want to make a point here. So, these charts are conceptual and they're not intended to reflect the specific contents of a profile. The NIST framework intentionally leaves the contents of the profile open because your organization is going to want to tailor it to meet your needs and be most effective in your organization.

Now we're going to talk about establishing or and improving a cybersecurity program. So it's not just a one thing that you do at the beginning, it's a something that we continue to do to improve our program. So step one is to prioritize and scope. And here we identify the business and mission objections and our priorities. And then we make decisions regarding cybersecurity that support the business line of process. Step 2 is called Orient. And in this step we identify related systems and assets and our overall risk approach. We consult sources to identify threats and vulnerabilities, those inside-outside the organization.

Step 3 is to create a current profile. That's what we just discussed in our previous slide with the graphics. Again, this has to do with indicating the category and subcategory outcomes that are currently being achieved. And next we're going to conduct a risk assessment. In doing a risk assessment, we're going to be guided by the organization's overall risk. We're going to analyze the operational environment to discern the likelihood of a cyber event and the impact it could have. And then we're going to identify emerging risks and use cyber threat information from internal and external sources.

Step 5 is to create a target profile. Again it's like the graphic we went through. A target profile should appropriately reflect a criteria within the implementation tier. So when we're creating it, identifying it, writing it up, we want to make sure it does, you know, stand up with the description of what the tier is. And then step 6 we want to determine, analyze and prioritize gaps. It compares the current profile and the target profile to determine the gaps and then we create a prioritized action plan to address them.

And in step 7 we implement an action plan. We need to determine which actions to take and address the gaps, the ones that we see, and we decide that we're going to—well, that we have already decided that we're going to do. So, our organization could repeat these steps as needed to continually assess and improve its cyber security.

So, it's important to use the framework. It doesn't do us any good if we don't—if we go through this process and assess where we are but we don't go back and apply it to our organization. So, an organization can determine its activities that are most important to them. The framework can be applied to a system and used throughout the system's life cycle. This is really great because you can think of a large project and so the framework can be applied to that project and used

throughout the life of it. And again, the cybersecurity outcomes determined through the framework should serve as the basis for ongoing operation.

Okay, we'll do our activity. Which of the following is a correct statement: Your answer choices are: A, A tier represents the maturity level of the organization; B, Profiles always represent cybersecurity outcomes currently achieved; C, Outcomes from using the framework should reflect in operations; D, Self-assessment is a one-time step at the beginning of a cyber program. Please make your selection.

If you said C you were correct. It's important that outcomes are from the framework are applied back through your organization, otherwise the cybersecurity program is ineffective. If you said A, that was incorrect. Tiers are not maturity levels but they provide a context on how an organization views risks. B, if you said B, that was incorrect. There is, we use two types of profiles. We have a current profile and a target profile, so profiles are not just what's currently being achieved but it's also where we want to go. And if you said D, that was incorrect. Self-assessment is not a one-time thing; it's used every time the cybersecurity program is to be improved. And now I will pass it back to Bruce.

Bruce Eisenhart: Thank you, Ralph. The final learning objective we have for this module is identify the resources for information sharing. We're going to look at three key points here: What can you report or what should you report. What are some of the organizations you could get information from or report to? And finally, where can you go to get help if you're a victim of an attack.

What are some of the things to report? Well, you know, in the first line objective Ralph talked about some of the threats and some of those attacks that might happen to you or denial of service or malware, including ransomware. These things mainly have happened so far against IT systems, but there are attacks against operational systems such as traffic signal controllers that could have a safety impact and could include signal timing changes, blocked sensor calls, flash conditions: all things to consider as possible cybersecurity attacks that you'd have to investigate and if they are, then that'd be something you'd want to report. There are in the Student Supplement, there is this larger list of different types of attacks as Ralph mentioned in learning objective 1.

So where do you find information or report incidences? One of the things that have been set up is something called an Information Sharing and Analysis Center or ISAC. These are meant to help critical infrastructure owners and operators protect their facilities, personnel, and customers from cyber and physical security threats and other hazards. ISACs in general collect, analyze, and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance their resiliency. There are two key ISACs in the transportation sector. The one of most importance to people in traffic engineering is the Multi-state ISAC or MS-ISAC and the one for public transportation is the Surface Transportation ISAC or ST-ISAC. And I'll talk about both of these in the next couple slides.

The MS-ISAC is an effort of the Center for Internet Security, CIS, and the Office of Cybersecurity and Communications from DHS. It's actually funded by grants from (DHS) Department of Homeland Security. Its mission is to improve the overall cybersecurity posture of the nation's state, local, territorial, and tribal governments to focus cyber threat prevention,

protection, response, and recovery. The members of this are all 50 states have parts of agencies that are members of it. All fusion centers, and I'll talk briefly in a couple slides about what fusion centers are, and hundreds of local agencies. There is the URL for the MS-ISAC and this is the primary ISAC for people in public—or for people in traffic systems, traffic operations. Notice the one group that is not on that list is private companies. So vendors, people like that, cannot be a part of the MS-ISAC. It is just for the public sector.

What does the MS-ISAC provide? Well, you can find thread details on there. And this is a screen capture of a piece of their public facing website, so it shows they have a list of top ten, top malware from the last month that have been hitting the public sector. If you are a member, you can go in and see what the actual list is. This is just representative. They have a section on identified solutions to some of the malware. They also have a 24/7 system operations center for threat reporting. It has a phone number and or an email that you can contact them. They have a Computer Emergency Response Team or CERT that can come and help you if you have an attack and you need to respond and recover from it. At the moment, MS-ISAC is primarily focused on IT issues, not ITS equipment issues. So, if you went and looked at the top malware attacks you'd see malware that's going after IT systems. So, while this is the primary place the transportation agencies should look for, it is still covering mostly IT because that's where most of the attacks have been in even the transportation sector.

Now the other ISAC, the Surface Transportation ISAC or ST-ISAC, is actually a combination of three ISACs that existed previously: one for rail, one for public transit, and one for over the road bus. And that's a little screenshot from their website showing a bunch of rail arrival departure screens. It provides information through several different reports. They have a transit and rail intelligence awareness report, an over the road bus report, and an open source cyber report. You can submit an incident. They have an incident form. And there is the URL for the ST-ISAC. But again, this is focused more on the public transportation. It wouldn't be the first choice for traffic agencies if they had something come up.

I mentioned on the first chart talking about it, these fusion centers. Fusion centers operate as state and major urban area focal points for receipt analysis, gathering and sharing of threat-related data. They include fire and EMS. The primary contacts in your region are most likely public safety. If you want to learn more there are several places. There's a DHS has a list of all the fusion centers. And there's actually a fusion center association. They have a very broad area of responsibilities. Cyber is just one of their areas of responsibility. And if you had a cyber-attack it would be worth finding the contact and talking to them. They may or may not be involved in that. It depends on the area and whether that fusion center has a lot of work in cybersecurity or whether their work is primarily in physical security and other things like that. But check with your public safety contacts about that.

And finally, where to get help. There are two additional key resources that I'll mention here about where to get help if you have an attack. The National Cybersecurity and Communications Integration Center, NCCIC, has a 24/7 operations watch center. Now this is a DHS facility. The first one, the ISACs are not. They're funded by DHS but they're not DHS. They're run by a nonprofit organization. But this one, the NCCIS, is DHS. They have a cyber awareness incident response and management center and there's the URL to get to that. This was formed in 2009 and in 2017, got reorganized to merge the CERTs that I mentioned before into that. And, as an example, one of the key CERTs that would be involved with transportation response and

recovery is the ICS-CERT which stands for Industrial Control Systems Cyber Emergency Readiness. They do alerts, response teams, focus on recovery. They have online training. So if you want to get some training to help, you can get it from the ICS-CERT. Talk to people at DHS. They do in person training as well, so if you want to get some training for your agencies, there's a variety of ways to get that.

One final activity. Another multiple choice question. For the MS-ISAC, the main ISAC for Surface Transportation traffic agencies, which group cannot be a member of the MS-ISAC? State transportation agencies; municipal transportation agencies; ITS vendors; or county transportation agencies?

And the correct answer is ITS vendors. MS-ISAC only allows public sector members. In general, and so the state transportation, municipal transportation, county, ISACs also have a single person who is the primary contact. So, if you're a State (DOT) Department of Transportation there's a single person who's your primary contact. You're going to have to go probably through your IT organization to figure out who those are.

So that is our four learning objectives. To summarize the module, we started out with a discussion of the need for cybersecurity that looked at some key terminology, the scope of the problem and some of the key threats. The second learning objective started to get into the basics of the NIST cybersecurity framework covering primarily the core functions. The third, applying the cybersecurity framework, looked at the tiers and the profiles of the NIST cybersecurity framework and how they would relate to your applying it to your organization. And then, finally, we identified a few resources for information sharing.

So that is our presentation. We appreciate it if you would go and take the post-module evaluation and we hope that you provide us feedback that you have found this module interesting and informative. Thank you very much from both Ralph and I.