The White House

Office of the Press Secretary

For Immediate Release February 12, 2014

Background Briefing on the Launch of the Cybersecurity Framework

Via Conference Call

11:06 A.M. EST

MS. LUCAS MAGNUSON: Hi, good morning, everyone. We're just delighted today to launch the Cybersecurity Framework in an event at 1:00 p.m. This call will be to preview that event and the framework itself. Just as a reminder, the information in this call is embargoed until that event begins at 1:00 p.m. All information is attributable to senior administration officials.

With that, I will go ahead and turn it over for opening comments to senior administration official number one.

SENIOR ADMINISTRATION OFFICIAL: Thank you. Good morning, everyone. Thank you for joining us on this call. We're very excited to be here today. This is a major milestone achievement for us.

Just to set the context for the discussion, last year the President issued Executive Order 13636 on improving critical infrastructure cybersecurity. Some of you were probably on this press call a year ago when we launched the framework. But if you recall, that EO directed the administration to take three broad steps in partnership with critical infrastructure stakeholders in industry and in government. One was to improve information sharing with the private sector; two was to raise the level of cybersecurity across U.S. critical infrastructure by encouraging the adoption of cybersecurity standards and best practices; and three, to enhance privacy and civil liberties while undertaking these actions. The cybersecurity standards and best practices were to also be supported by the development of a voluntary program to encourage the use of the framework.

So working with and in partnership across government and industry, we have made significant progress in each of these areas. So today, exactly one year later, we are pleased to announce the release of the framework and the launch of the voluntary program. And from our perspective, this is really a very major turning point in cybersecurity discussions. We believe that from today on we'll have a new shared vocabulary about cybersecurity that will allow CEOs, boards of directors and policymakers -- not just here in the U.S., but around the world -- to set baselines and chart the course for improvement and actually make those improvements.

Both NIST and DHS have played incredibly pivotal roles in the development of these products and they've worked very diligently to deliver these efforts with quality and substance, and I should say, and on time -- which is a major achievement as well -- and in a manner that is responsive to industry's needs as well.

So with that, I'm going to turn it over to senior administration official number two to discuss the Cybersecurity Framework.

SENIOR ADMINISTRATION OFFICIAL: Thank you, everybody, and I want to thank everybody who's joining today's call. So my role is to discuss version 1.0 of the NIST framework for improving critical infrastructure cybersecurity. A year ago today, the President issued the executive order calling on NIST to convene with the private sector to identify a set of industry standards and practices that could help organizations that are managing cybersecurity risks. That executive order was an important step to raise consciousness among the broader business community and initiate a public-private partnership on a national scale to protect our critical infrastructure and supporting structures.

The 39-page Cybersecurity Framework document and its accompanying road map represents the beginning of

LATEST BLOG POSTS

February 14, 2014 12:00 AM EST

West Wing Week 2/14/14 or, "The Red, White, and Blue -- and the Blue, White, and Red"

Welcome to the West Wing Week, your guide to everything that's happening at 1600 Pennsylvania Avenue.

February 13, 2014 2:05 PM EST

Making the World Safer from Pandemic Threats: A New Agenda for Global Health Security

The Global Health Security Agenda is an international effort to enhance our ability to prevent, detect, and respond to outbreaks of infectious disease threats.

February 13, 2014 1:38 PM EST

President Obama Speaks to the Latino Community on Why it is Important to #GetCovered

President Obama records a video message to help educate Latinos about the benefits and protections under the Affordable Care Act and encourage them to sign up for health coverage. Check out the message and hear the President talk about the tools available to help you and your "amigos, familia and vecinos" #GetCovered

VIEW ALL RELATED BLOG POSTS

STAY CONNECTED

Facebook YouTube

Twitter Vimeo

Flickr iTunes

what I hope will be a continuing, common-sense conversation about how to protect these critical assets. One of the biggest cybersecurity issues facing critical infrastructure companies in all of these sectors -- transportation, financial, health care, communications, energy -- is simply this: When are you doing enough? When do you know you've done the best you can to protect your company, your suppliers, your customers from the adverse effects of cybersecurity threats?

As technology and innovation drive increase complexity in our daily lives, coupled with a collection of threats that are increasingly varied and changing -- that includes criminal gangs in foreign countries to disgruntled insiders -- doing your best in cybersecurity can, frankly, be quite overwhelmingly for many organizations. So NIST's approach to our charge in the executive order was to adopt a partnership and collaboration approach. So working with industry we've developed a structure that any company, large or small, and any one of the very critical infrastructure sectors can voluntarily use to make improvements in their current cybersecurity systems or to create a credible cybersecurity approach if they don't already have one.

The key message is that cybersecurity is not something you just put in place and walk away. There's no prescription or magic bullet for cybersecurity. There are only well conceived, proven ways of continuously managing the risk.

The other key message today is that we wanted this framework to be voluntary. And that was important because it encourages the widest possible set of stakeholders to come to the table and work with us. It also ensures that the muscle in this approach comes from the companies themselves. Voluntary standards are a tradition in the United States because they work. When industries get together and determine for themselves what standards describe a quality of a product, these standards are much more likely to be adopted quickly and implemented fully.

The heart of this process was to listen to industry to be sure we knew what industry needed from this framework. So we held five workshops around the country with thousands of participants. We provided draft versions of the framework and supporting material multiple times at our website. We encouraged comments on the draft, and we carefully considered all of the feedback we received.

The result is a flexible tool that allows diverse industries and stakeholders to talk about and describe how they would take actions to improve cybersecurity. It lays out the critical elements of any cybersecurity program and then links those elements to proven standards and protections for companies to consider using. The framework describes the key functions of cybersecurity as identify, protect, detect, respond and recover. And then it further describes categories and sub-categories of actions a company can take to carry out those functions.

And finally, it offers a list of known publicly vetted standards and practices that address these categories. By relying on those practices already proven and used throughout industry we can focus on the more pressing problems instead of driving apart an already fractured system of standards, regulations, policy and law.

We can also say definitively, based on the large number of companies both in critical infrastructure and in the broader economy that have suffered losses in revenue and business productivity in the last year, it is time to try something new.

So what we've done, what's really new, is we've integrated many complement pieces that organizations need to address cybersecurity risk management in a way that makes it easier to implement a strong approach. And we've done it in a way that it's accessible to a broad audience of stakeholders -- because it's really critical that all levels of an organization, all the way from the top in the C suite down to the construction supervisor, they need to understand how and why they protect their company from cyber threats.

The new framework does three important things. First, it jumpstarts a vital conversation between critical infrastructure sectors with the various regulatory authorities related to them about what cybersecurity issues they have in common and how these issues can be addressed cost-effectively and voluntarily without reinventing the wheel.

Secondly, it provides a consensus description of what's needed for a comprehensive cybersecurity program, and in the process provides a powerful tool for companies to seek competitive advantage by improving cybersecurity and lowering risk.

And finally, it helps companies prove to themselves and to their stakeholders that good cybersecurity can be the same thing as good business. By mapping their individual cybersecurity programs against the full list of functions, categories and specific standards a company can identify gaps and tailor improvement plans to their specific needs. And we hope they will create metrics that document those improvements.

Some smaller companies may discover in the process that their entire cybersecurity effort consists only of passwords and anti-virus software with no real-time detection capability, even though automated tools are widely

available and affordable. Another example could be a larger company may find that the framework is a useful tool for holding their cybersecurity contractors accountable, or for purchasing these services in a more systematic way in the marketplace.

The bottom line is that we all need an agreed upon way to talk clearly to one another about cybersecurity issues and solutions and to hold each other accountable. And this is really the start of that conversation. I'm looking forward -- all of us at NIST are looking forward to continuing to work collaboratively with industry and government to lower cybersecurity risks so we can better protect our economy and our national security.

Let me turn it over to senior official number three.

SENIOR ADMINISTRATION OFFICIAL: Thank you. And let me add my thanks to all of you on this call for your interest in this. As you know, our nation's critical infrastructure, both physical and cyber, is the backbone of America's national security and economic prosperity. But that infrastructure faces a variety of risks to its functionality, including acts of terror, natural disasters and cyber attacks. And because the majority of our national critical infrastructure is owned and operated by private companies, both the government and the private sector have a shared responsibility to reduce the risks to that critical infrastructure.

To address these challenges, the President issued not only the executive order on improving cybersecurity critical infrastructure a year ago today, but also Presidential Policy Directive 21 on Critical Infrastructure, Security and Resilience. Today, the Department of Homeland Security and its colleagues at the Departments of Commerce and Energy will talk about the very real and tangible steps that we have taken to implement the executive order and the PPD.

The executive order directed the Department of Homeland Security to establish a voluntary program for critical infrastructure cybersecurity, to serve as a federal coordination point for cybersecurity resources, and support increased cyber resilience by promoting the use of the framework that was developed under the leadership of NIST.

DHS is announcing this afternoon the creation of that program, which we call Critical Infrastructure Cyber Community -- or C-Cubed -- Voluntary Program. The C-Cubed Voluntary Program stands for Critical Infrastructure Cyber Community, but it also emphasizes another three c's: convergence, converging resources to support cybersecurity risk management and resilience through the use of the framework; connecting critical infrastructure stakeholders to the national resilience effort through cybersecurity resilience advocacy, engagement and awareness; and, finally, coordinating critical infrastructure cross-sector effort to maximize national cybersecurity resilience.

The C-Cubed Voluntary Program represents a long-term goal for cybersecurity, encouraging organizations of all sizes to establish or improve their cyber risk management processes, and to take advantage of available resources made available by the United States government.

For example, the program supports the use of the Cybersecurity Framework through the Cyber Resilience Review, CRR. The CRR is an assessment to evaluate an organization's information technology resilience. The CRR may be conducted as a self-assessment or as an in-person, facilitated assessment. The goal of the CRR is to develop an understanding and measurement of key capabilities to provide meaningful indicators of an organization's operational resilience and their ability to manage cyber risk to their critical services during normal operations and at times of operational stress and crisis.

To date, DHS has conducted more than 330 CRRs at the request of critical infrastructure entities nationwide. The inherent principles and recommended practices within the CRR align closely with the central tenants of the Cybersecurity Framework. Organizations can use the CRR to conduct an analysis of their current practices and how they compare to the principles of the Cybersecurity Framework.

DHS also currently offers a range of other cybersecurity resources to public and private sector organizations, including information on cyber threats and vulnerability; cybersecurity incident resources such as through the National Cybersecurity and Communications Integration Center, or the NCCIC; or the U.S. Computer Emergency Readiness Team, the US-CERT; or the Industrial Control Systems Computer Emergency Response Team, the ICS-CERT.

We also have software assurance programs and other technical resources, such as cybersecurity strategy development, cybersecurity assessment tools, cyber exercise planning, cybersecurity risk management training, cybersecurity resilience review, a national vulnerability database, and road maps to enhance cybersecurity in certain specific sectors.

Speaking of our sectors, DHS will work with sector-specific agencies and other federal agencies to identify the

suggested offerings and provide assistance best suited to address a particular sector's industry capability gaps. For example, the NIST Cybersecurity Center of Excellence plans to work with owners and operators to develop sector-specific use cases that build out security platforms based on the framework and existing standards and best practices. And the Energy Department is offering guidance and assistance through their program that supports the energy sector cybersecurity capability maturity models, or C2M2.

The C-Cubed Voluntary Program is an innovative public-private partnership led by DHS to help align critical infrastructure owners and operators with existing resources that will assist their efforts to use the Cybersecurity Framework to manage their cyber risks.

We've already seen strong interest from the private sector in partnering with us on this effort, and it aligns closely with the partnership effort reflected in the National Infrastructure Partnership plan 2013 -- 2013 Partnering for Critical Infrastructure Security and Resilience.

It boils down to this. In cybersecurity, the more systems we secure, the more secure we all are.

SENIOR ADMINISTRATION OFFICIAL: Thank you. And I just wanted to hit on two other topics as we move forward. One is what's happening with the regulatory environment and then what's happening with the incentives that we've been working on developing.

With respect to the regulatory environment, I just want to be clear that for the administration, the goal is not to expand regulation. Rather our goal is to streamline existing regulations wherever possible and to bring those regulations into alignment with the framework. So, to that end, executive branch agencies are reviewing their existing regulatory or voluntary programs in this area. And then in May of this year, consistent with the executive order, these agencies will also propose prioritized risk-based efficient and coordinated actions to mitigate cyber risk.

We're encouraging those agencies to focus on voluntary efforts and programs to support adoption of the framework. For those sectors where regulations already do exist, agencies could engage in existing rulemaking processes to support efforts to harmonize and align current regulations with the framework. And we have invited our independent regulatory agencies to follow the same process.

And then we are continuing to work and develop incentives to encourage the use of the framework in coordination with both NIST and DHS. We do believe that developing incentives around a framework is a key endeavor and we intend to keep moving forward with this process, and it's going to be done in partnership and engagement with industry.

Back in 2013, we released a potential set of incentives that we intended -- that we said at the time that we'd review further, and that's what we've been working on. The relevant agencies have further defined the scope and path forward for some of those incentives, including technical assistance and process preference, cyber insurance, grants, cost recovery, public recognition, regulatory streamlining and government procurement.

As these plans develop, they'll be shared publicly over the next few months and will include details on how to get engaged in the process.

However, I do want to say that we believe that the best drivers for adoption or use of the framework will ultimately be market based. Don't get me wrong, I think the government-based incentives are really important for us to pursue. But at the end of the day, it's the market that's got to drive the business case for the Cybersecurity Framework. The federal government is going to do its best to make the costs of using the framework lower, and the benefits of the framework higher, but it's the market that's going to ultimately make this work.

So, with that, I will close.

Q My question is, first of all, can you point to a couple specific things that would encourage companies to adopt these voluntary guidelines or best practices aside from that specific regulatory agency synchronizing their regulations with the framework? And then, secondly, some experts have told me that they felt that this set of standards embraces the status quo to a large extent. Is there flexibility for these things to be updated as new threats or industry best practices change?

SENIOR ADMINISTRATION OFFICIAL: I'm happy to answer that question. I think the question on why an organization looks to adopt and use the framework stems from, in many respects, enlightened self-interest. There's a couple of key things. One is the framework explicitly makes the tie to risk management. And so protecting the information in these organizations, protecting how that information is used to provide critical infrastructure services, is something all of these companies want to do. It's very much in their interest to know how to adopt what's considered best practice and to put it in a framework where it can be effectively used.

The other benefit actually comes from the fact that since this is a shared infrastructure, it gives them great advantages of scale where there are dependencies. The contractors that they depend on -- there's a common way of defining how they support the overall cybersecurity effort. It means that they can turn to services and vendors to provide security services and security products. And those are very powerful reasons why companies are looking at this and I think you'll be seeing that in the days ahead.

With regard to the continuous improvement, I would say it's twofold. It's actually in the process itself. The framework defines ultimately the risk management and continuous improvement cycle within companies. In fact, the tiers describe increasing levels of maturity in that approach, where you become more self-aware and more self-improving all the time as you adjust your profile to changes in technology. But also the framework is designed to be continuous.

We do not consider this to be done. One of the road map documents that's being released today describes the steps we are going to continue to take to support the framework. We think the bringing together of all of these industries to work and update and address gaps and improvements is essential to this overall approach. This is a living framework.

Q Thank you very much for taking my question. Regarding the metrics, is there going to be any effort to place any consistency in the metrics by which private sector adopters measure their conformance to the framework? If there is consistency, then how can you assure the adopters that they won't be held liable for adoption of the framework?

SENIOR ADMINISTRATION OFFICIAL: It's a great question. And as you know, it's been a very active area of discussion throughout the entire framework process. The way the framework is laid out has each individual organization developing a profile and using that profile to identify next steps. So the metrics are really internal and unique to the organization that's adopting.

As this gets used and you start looking at dependency, there clearly will have to be some shared understanding of how to approach the issue of metrics. And that's already been identified by the companies working with us as something that they would like to continue to work on in the next version of this framework as well.

So I would consider that the metric discussion is one that's going to mature over time. Remember, this is explicitly a voluntary program, and so it's really about companies setting their own level of care, not having some one-size-fits-all approach from the outside.

Q Hey, everybody. Thanks so much for doing this. I just want to look at the congressional picture here. It's always been the case that the administration has said it has to go back to Congress to fill in quite a good number of holes, whether it's on information sharing, or on the issue of incentives, or so forth. So what should we expect from the administration going forward when it comes to these very unresolved issues that remain with the framework?

SENIOR ADMINISTRATION OFFICIAL: Well, I think a couple of things, one of which is I think we believe that the framework stands on its own and can be an incredibly powerful tool for enabling the kind of conversations that need to happen between CEOs and boards, and between the government and industry. So we think that regardless of what happens between the administration and the Hill and up on the Hill, the Cybersecurity Framework is an incredibly powerful tool that we can leverage to make real improvements across our critical infrastructure regardless of what happens from there.

Of course, we do believe that we continue to need to engage with the Hill, and, in fact, we have. We've briefed congressional staff on the framework and have gotten a lot of really good support from both sides of the aisle. And you'll see some of that in some of the quotes that come out later today from some of our congressional engagements as well. But I do think that the administration will continue to engage Congress on improving our ability to do information sharing, on updating the statutes that govern how we actually do cybersecurity within the federal government, DHS's authority in this space. All of our legislative agenda will continue. But none of that I think detracts from the fact that the framework is going to be a really significant advance in critical infrastructure cybersecurity.

Q Sure, can I just quick follow? I just wanted to clarify something. This is a very different approach than what the administration had thought in legislation as far back as 2011 and 2012, when there was what seemed to be a greater belief that regulation was the way to do this, or a more regulatory-minded approach was the way to bring about these changes in cybersecurity. And that led to a huge debate between businesses who just didn't like that, but the administration seemed to feel very strongly about it. So when you compare where you guys were in 2011, 2012 versus now, what has you more confident that this approach is going to produce the right changes in cybersecurity?

SENIOR ADMINISTRATION OFFICIAL: Well, I think what gives me a lot of the confidence is the degree of engagement with industry that has happened over the development of the Cybersecurity Framework. We have had just an unbelievable level of participation that NIST can speak to in greater detail, and an enormous participation from across a huge range of companies both in terms of the sectors that have been involved as well as the size of the companies that have been involved.

And because of the result of such a participatory effort, that really points at what is the acknowledged set of best practices and standards in this space I think it really does become kind of the gold standard for how to approach and talk about cybersecurity -- not just for our critical infrastructure, but for any organization that wanted to use the framework as a way to tackle its cybersecurity problems. And so that's what gives me great confidence that this document will be both usable and relevant to the organizations actually trying to do cybersecurity.

Q I have two quick questions. Do you have a cost estimate of what the current cybersecurity threat is here in the United States? And also, how can we get a copy of the framework?

MS. LUCAS MAGNUSON: I'll answer the second question first just quickly. The framework will be online a little bit before the 1:00 p.m. event, and we'll have links to that in a press release that we plan to send around that time. So everyone will get access at the same time.

And on question number two --

SENIOR ADMINISTRATION OFFICIAL: I think that getting a cost estimate on exactly what the cyber threat actually costs the United States on an annual basis is incredibly difficult, especially because a lot of people never report that they've been hacked. Companies don't report that; individuals don't report that. And then, even a lot of times assessing what the value of the damage that's been done or the information that has been stolen is incredibly difficult to do.

For example, it's often very difficult to put a price tag on intellectual property that you've never even brought to market yet that's been siphoned off and taken to a competitor, for example.

So I think it's very difficult to provide cost estimates with any sort of fidelity in there. But we know from the scope of activity that is reported, from the scope of activity that we can see, that the numbers are very large and that this is a very real and significant problem to a lot of businesses and individuals, as well as the government across the country.

Q Is there a range of numbers then? And also, does the framework include any sort of suggestion or incentive for companies to report to the government when they have a loss?

SENIOR ADMINISTRATION OFFICIAL: I think that even getting into ranges is just a very -- it's such a squishy territory and art that I just don't even think that that's a viable conversation to have.

In terms of encouraging the reporting, I don't think that's really -- the framework is not really aimed at that. What the framework does point to is it says that you need to think about not just the protection part of cybersecurity but also the response and recovery part, meaning that you will face incidents as a company, no matter how good your protection and detection capabilities are, so you need to be prepared to be able to respond when you detect an incident, and you need to be able to recover from that. Now, in the process of figuring out that you need to be able to respond and recover, that encourages more companies to be more proactive, that would be a side benefit, but it's not really the driver behind the framework.

SENIOR ADMINISTRATION OFFICIAL: We think that voluntary programs also may help encourage companies to come forward simply by giving them information about who to call and how to come forward. And so putting up resources about the NCCIC and the US-CERT and ICS-CERT, for example, may help facilitate some of that interaction and sharing of information.

Q Just getting back to incentives, so what can the administration or the executive branch do on its own without going to Congress for legislative proposals? And then, what specifically would you want to see from Congress in the area of legislation related to incentives? I realize you said that you expect the market to be the driver here for the most part, but still, I think people are looking to see what can the federal government do both from the executive branch standpoint and the congressional point of view.

SENIOR ADMINISTRATION OFFICIAL: Well, I think that in multiple areas, there's actually a fair amount the executive branch can do on its own. For example, we've been engaged in very serious discussions with the various insurance companies to talk about what's needed to actually get a cyber insurance market really thriving. Public recognition efforts, even talking in the field of cost recovery, that's often done at the state level, and that involves a lot of discussion with regulators both at the federal and state level, not even necessarily going back to

Congress. So there's actually a broad array of what we want to pursue in that space.

In terms of what we actually want from Congress, I think that's actually something that we're still working on. I think that's actually something that, particularly as we work on the incentives and as companies begin to use the framework, that we actually want to get a better sense of what incentives would really matter and then what of those incentives are really, in fact, actually held back by some sort of statutory limitation, that congressional action would actually be beneficial in changing or enabling something to happen.

So it's no surprise that legislation doesn't move very fast through Congress right now, so I don't think that we are hinging our strategy in this space on congressional action, but we'll get back there when we think it's necessary.

Q Just one quick follow-up on what you guys can do on your own -- and maybe this will come out in the coming months -- but just, again, when it comes to federal procurement policy, sort of embedding some of these best practices and standards in what is being supplied to you, somehow requiring that in your acquisition processes. I don't know if you can speak to that.

SENIOR ADMINISTRATION OFFICIAL: Well, I think that if you take a look at what was in that report, the joint report produced between the Defense Department and GSA, it really outlines how we can start to bring cybersecurity requirements more into our acquisition process across the board. And I think you will see us continue to do that. Just as the private sector is, the federal government is under enormous pressure from cybersecurity threats in all sorts of directions, and so I think we're going to be exploring how to do that and how to put that report into practice.

But, of course, there are other things that we can do in the technical assistance side and in other areas that you'll see even starting today with the voluntary program launch.

SENIOR ADMINISTRATION OFFICIAL: As was noted earlier, there's an enlightened self-interest here that we're counting on with regard to businesses' interest in improving their cybersecurity. And part of making that business case is providing information to inform their risk assessment. And so there's been a great deal of work done to reach out to the various critical infrastructure sectors to make sure they understand the nature of the threat, vulnerabilities and consequences.

SENIOR ADMINISTRATION OFFICIAL: A lot of these steps are going to be outlined in the road map itself, how we're going to look at the government side of this in the context of the framework.

Q I wanted to ask how you plan to track the success of the program or how widely adopted these standards are, or how widely adopted the framework is going be? And also, one of the experts, or a couple of the experts I spoke with mentioned a concern that the framework was over-focused on privacy and data security, not as focused on sort of the industrial interest, particularly safety and kind of resilience of the physical infrastructure. Can you address that as well, please?

SENIOR ADMINISTRATION OFFICIAL: On the tracking of success
of adoption, we may not ever know how widely the framework has been adopted, because obviously there's no requirement for companies to tell the government that they're using the framework to improve their cybersecurity.

But we are hoping through the C-Cubed Voluntary Program to be able to have some interaction with companies that are looking for assistance in adopting the program. We also are designing a way for companies to provide us with feedback on how helpful the C-Cubed Voluntary Program is for them so that we can continue to improve that program. And we'll be working closely with NIST to make sure that they're getting the feedback on the framework itself. So that will hopefully give us a sense of -- certainly of how useful it is, if not how widespread the adoption is.

SENIOR ADMINISTRATION OFFICIAL: Yes, I think that's right. I think a lot of the adoption that you're going to see is going to be evident as these companies push this into the market, into their practices. I think you're going to hear a lot of companies talking about this. You're going to see it in business-to-business relationships in a whole host of other ways. And so there will be a lot of indicators about activity -- and also, in the participation of these companies as they come back and work to improve the framework process, because, remember, a key part of that is looking at what are the things we're learning as we're using this. And so we're expecting these active participants to be working with us as the framework improves.

With regard to the balance, this is something that the framework process has dealt with all along. We've been very careful to reflect comments like that in the public and to react to those. We think we've really taken that seriously, and we hope that the overall consensus is that this is a very balanced document. Remember, a lot of these issues -- whether it's data privacy and security, whether it's industrial controls -- are designed to be integrated into the framework approach. There are things that come out as an organization looks at their own structure through the profile and defines this.

And so you have to be a little bit careful that you're not looking at the top-line framework and the language that is there as the overall barometer of how committed we are to this or to that. It really does come out as you apply the framework. And we think the balance is pretty good.

Q This is on federal procurement. You said that vendors who adopt the framework might stand a better chance of winning contracts. The earlier version seemed to encourage incident reporting as part of an effective response. That's new for a lot of contractors who are outside of the defense industry. So I'm wondering how the government might help them implement that part of the framework.

SENIOR ADMINISTRATION OFFICIAL: So I think that really that's kind of -- part of the reason that we're creating a voluntary program is because one of the themes that has clearly emerged is oftentimes a confusion about if you do have a cybersecurity incident, who do you reach out to? Who can you call? And in fact, we're trying to make sure that there is no wrong door for coming into the federal government, and that wherever you come in we can get you to the right place, to the right people that should be able to help a company deal with a particular incident, whether it turns out to be one that they want to deal primarily as a mitigation exercise and work with DHS, whether it's a criminal activity and it's in the lane of FBI or Secret Service. But really what we want to do is encourage companies to be able to get to the right information so they can figure out who they can call on that.

Q I understand that the Appendix B on privacy has been removed, it won't be in this first version. Can you talk a little bit about how the privacy issue is addressed throughout the document?

SENIOR ADMINISTRATION OFFICIAL: Sure. In response to a comment we received through the process, the section on privacy has not been removed as much as integrated into the framework. And so stakeholders have always and consistently identified privacy needs as essential to this framework. There was not support, or there was certainly not sufficient support for a standalone Appendix B. We received comments that it needed to be integrated and so, in response, that has been integrated into the main body of the framework and into its core.

Q I'm wondering what's next in terms of how does a company actually join the program and when? And then, to follow up on the measuring success piece, how many companies are you expecting to or hoping will join the program? And you talk about raising the level of security. How do you measure that, and will this program make critical infrastructure more secure?

SENIOR ADMINISTRATION OFFICIAL: On your question of how to join the program, really it's as simple as visiting the website. And we're going to have a very easy entry point at dhs.gov, and then more detail at a link through that to us-cert.gov.

And there's no magic –- you don't have to sign up, you don't ever have to let us know even that you've been to the website. But if you would like to avail yourself of some of those resources, again, we're going to make it very easy for you to know how to do that and how to interact with the folks in the government who might be able to provide varying degrees of assistance in this option of the framework.

SENIOR ADMINISTRATION OFFICIAL: Let me just also point that there's –- just for clarification, there's the voluntary program, which is I assume what you're referring to in the program. But the framework itself can be used by organizations, independent of whether or not they're participating in that program. Those are decisions being made. Internal to these organizations, based on feedback, we're expecting rather widespread use of this right away. We know that organizations are looking at this seriously.

So I didn't want you to be confused about using the framework within an organization and participating in the C-Cubed Voluntary Program.

Q Sorry, the part about the measuring success piece?

SENIOR ADMINISTRATION OFFICIAL: So, again, I think the success of -- well, again on the program side, the program is designed to support use. So I think the real test of that is going to be are we doing things that -- are we providing tools and resources and things that support organizations of all sizes, of all different backgrounds, to put this framework into use.

On the framework itself, we're going to measure success by is it being put into practice; is it driving these improved cybersecurity behaviors that lead to better outcomes. And that's something we're going to see and continue to work on extensively as the framework process continues.

Q Thanks very much. I wanted to tag back to something that bachelor number one -- I mean, administration official number one said at the very end there about the regulatory environment. Can you talk a little bit about what agencies are doing as they're reviewing the current regulations and how they're going to update them? Can you give me a sense of the process behind that?

SENIOR ADMINISTRATION OFFICIAL: Well, of course, it varies depending on which executive agency you're talking about. But I think really -- they're engaging in their normal processes they have to engage with their stakeholders and with how they do their oversight process in their various sectors. And they're taking a look at whether or not they have cybersecurity regulations or requirements, guidance -- there's all sorts of names for it -- how that currently stacks up, how that stacks up against the framework, and then how to move forward from there.

So I think it really -- it varies a lot depending on the particular sector and agency that's involved. That work is going on right now across the different regulatory agencies.

SENIOR ADMINISTRATION OFFICIAL: Also they've worked with us throughout the entire process.

Q So DNI James Clapper was on the Hill yesterday to discuss major threats facing the nation, and one of them that he pointed out was vulnerabilities to the supervisory control and data acquisition programs. These are programs that run a lot of areas of critical infrastructure. And I'm wondering if you can address how the framework handles some of those vulnerabilities.

SENIOR ADMINISTRATION OFFICIAL: I'd be happy to. So the framework includes standards and approaches for SCADA and other industrial control systems. This has been a key part of the process from the very beginning. And so we agree. This is obviously something that many critical infrastructure sectors deal with. And it was important that it integrate both what you would consider traditional IT-type infrastructure in the organizations, but also dedicated industrial control-type systems.

So, again, it's most clear when you get right into the profiles and look at the underlying categories, sub-categories and references, but it's quite integrated in the approach. And again these organizations have worked with us all the way through. In fact, standards organizations were immediately responsive in aligning what they've been doing as part of the framework process.

So I'll end there.

MS. LUCAS MAGNUSON: All right. Well, thanks, everyone, for joining. Just a couple of reminders here before we close. The event will begin here -- the launch event -- it will be live-streamed on whitehouse.gov starting at 1:00 p.m. This call and the information is embargoed until that time. Again, all of the information is attributable to senior administration officials.

Right before the event begins at 1:00 p.m., we'll have a press release from here. And some of you have also asked about what others are saying about the framework, and we'll be distributing some of the comments that we've received from the private sector and others for your information.

And with that, I'll just thank you all for joining and we appreciate your time this morning.

END
11:57 P.M. EST

Refinancing
Rural
Service
Seniors & Social Security
Snapshots
Taxes
Technology
Urban and Economic Mobility
Veterans
Violence Prevention
Women

Mobile Apps

WWW.WHITEHOUSE.GOV

En español | Accessibility | Copyright Information | Privacy Policy | Contact
USA.gov | Developers | Apply for a Job