**ASPR June Hospital Preparedness Program Recipient Webinar Transcript**
*June 14, 2023*
*Call Transcript*

00:00:02.320 --> 00:00:07.369

**Heller, Matt:** I will now pass it over to Dave Csernak and Angela Krutsinger, who will open today's call

00:00:09.610 --> 00:01:18.069

**Angela Krutsinger:** Thank you so much, Matt. Thank you all for joining us today. We have Dave Csernak, Acting Regional Supervisor on the line, and I'm Angela Krutsinger, Acting Regional Supervisor. Before we hand it over to our first presenter, I would like to provide a brief overview on what we will cover today. Next slide, please.

As for our agenda, first, we will begin by providing a few updates relating to ASPR's Health Care Readiness Programs. Next, Bob Bastani, the Senior Cybersecurity Advisor to the Office of Critical Infrastructure Protection, will provide an overview of HHS-Sector Risk Management Agencies, or SRMA strategic objectives. Next, Rachel Lehman, the Acting Director of ASPR TRACIE will provide an overview of ASPR TRACIE's cybersecurity tools and resources. Finally, we will leave some time at the end for questions from the audience. Next slide, and I'll turn over to Dave.

00:01:20.340 --> 00:05:07.499

**David Csernak:** Thank you, Angela, and good morning…good afternoon to everyone on the line today. We'd like to begin today's webinar with a couple of administrative updates. Next slide, please.

Alright, starting off with the MRSE or the "Medical Response and Surge Exercise" update. The MRSE Design Team has made a number of updates to the MRSE and its supporting tools starting in Budget Period 5. The updates include: the layout of the Exercise Planning and Evaluation Tool, a streamlined version of the Surge Estimator Tool incorporated into the MRSE, simplified required patient tracking data inputs, qualitative questions on health equity considerations, a qualitative question to document roles and activities of important MRSE participants, and optional guidance to support HCCs in more fully including additional, non-core HCC members in the exercise. The updated MRSE Exercise Planning and Evaluation Tool, Situation Manual, and Evaluation Plan will be rolled out in July 2023 as part of a national webinar. Next slide.

Okay. The National Health Care Preparedness and Response Capabilities pre-decisional draft review has been extended, so as many of you know, ASPR is currently updating the Health Care Preparedness and Response Capabilities to reflect insights learned from recent disasters, and now we are at a point where we are soliciting your feedback and input as part of our pre-decisional review. We know many of you participated in the discussion leading up to the development of the pre-decisional draft, and now we welcome your review and feedback. We extended the deadline for comments until this Friday, June 16th. You can view the pre-decisional review draft and access the Online Comment Matrix to submit your comments using the links we will share in the chat. Thank you so much, Matt. And next slide, please.

All right, the updated ASPR organizational structure. So, as you might remember, last time we met, we discussed ASPR's updated organizational structure, and we want to quickly to revisit these updates. Under the updated organizational structure, the National Healthcare Preparedness Programs was elevated from a branch to an office and renamed the Office of Health Care Readiness. This is an exciting elevation within ASPR's organizational structure and is a result of the growing emphasis on the importance of health care readiness. We've heard concerns that HPP or other programs may be going away with this new org structure. This is not the case. In fact, our name change and elevation to an office, results in more attention and focus on our programs. This is a good thing! On the screen, you see the ASPR's new org chart to the left, and on the right, you see the Office of Health Care Readiness in more detail. We've broken down our major capabilities as well as our programs and activities. As you can see, there have been no major changes to our programs and activities. Rest assured, our partners will continue to be our priority and we look forward to growing our partnerships with all of you. We will now pass it over to Bob Bastani to discuss an overview of HHS-Sector Risk Management Agencies strategic objectives. Next slide.

00:05:15.000 --> 00:05:25.770

**Heller, Matt:** And Bob, before you start, there's a question in the chat that asks if the office is within an office? To answer this, the Office of Health Care Readiness is in the Office of Preparedness.

00:05:27.240 --> 00:05:58.909

**David Csernak**: That is correct. So, the Office of Preparedness is an executive office within ASPR which is led by a Deputy Assistant Secretary, Deborah Kramer, and the Office of Health Care Readiness is an office within that office. I hope that makes sense. All right. If there are no other questions, we'll turn it over to you, Bob.

00:06:00.720 --> 00:32:31.860

**Bob Bastani:** Good afternoon. Thank you for this opportunity to speak with you. My name is Bob Bastani. I am a Senior Cybersecurity Adviser in the Office of Critical Infrastructure. Protection in ASPR. Next slide, please.

I'm going to talk to you a little bit about the critical infrastructure concept and the concept of sector risk management agencies. I know some of you might be familiar with it, but some of you might not be, so we will cover that a little bit. And then we talk about the cybersecurity challenges and threats in health care and public health. We will spend a little time introducing you to how ASPR is structured to do its duty as this SRMA for the Healthcare and Public Health Sector. And then I'll talk to you a little bit about major cyber-led efforts in 2023, that are happening right now. Next slide, please.

So, there are 16 critical infrastructures and 16 sectors that have been identified by the United States Government as critical. They are critical to the national security, they're critical to economic and public health, and critical with safety consequences. Health care and public health is one of these 16 critical infrastructures. For each of these critical infrastructures, an agency has sort of been put in charge of looking after these infrastructures, and I'll talk to you a little bit about what that means. At a high level, these agencies are monitoring the risk that these the sectors face and then develop this mitigation strategy so that the sectors are not impacted, and the impact is minimal. The definition of the critical infrastructure sectors originally came through a Presidential Policy Directive, PPD-21. But very recently, in FY 21, it was codified in the National Defense Authorization Act. So, with the NDAA, it is now part of the law and structure of the critical infrastructure as a duty. These are very much defined in the NDAA. As I said, the Healthcare and Public Health Sector is designated a critical infrastructure. Next slide, please. I'm sorry, before we go there, if you can go back just really quick before we get to this. So, as I said, Healthcare and Public Health is, this is the critical infrastructure. So, HHS has been designated as this - what they call a “Sector Risk Management Agency.” These are the agencies that have been put in charge watching over these sectors. For Healthcare and Public Health, that is HHS. The HHS Secretary has designated ASPR to have that role, and within ASPR, the Critical Infrastructure Protection division has been put in charge of the duties of an SRMA. I’ll talk to you a little bit later about what that means. So, since we are talking about cybersecurity, you can go to the next slide, please.

All SRMAs are looking at the risks that these sectors face from all hazards. Increasingly, one of those hazards is cybersecurity and cyber threats, and for health care, that has been a growing and pervasive issue. And we've seen an increasing number of cyber-attacks against health care and you're seeing a destruction of service on a continuous basis. Unlike other hazards, for example, hurricanes, there is a season, although that season is getting longer and longer, cybersecurity seems to be an ongoing hazard that never ends. So, there are multiple reasons that are driving this pervasiveness and the increasing frequency of cyber-attacks.

First of all is sophistication. The cybersecurity attacks have become very sophisticated and the tools that the attackers use are sophisticated, and the attackers have a community, a very strong community that share information among each other, very effectively. So that strong community and this sophistication of attack types makes it more difficult to identify the attacks.

The other issue that that sector faces is the existing of legacy systems. For the longest time, health care and public health, in terms of systems and updates, was very stable. And as the technology moved, a big segment of the sector did not go through updating and upgrading. So, we face an existing IT systems legacy, tools, and so on, that some of them are running operating systems that are no longer supported by vendors. In some instances, there are systems, and the vendors are no longer there, which that really creates an opportunity for the attackers. And we see a lot of those systems being compromised.

On the other side, we also see the emergence of technology. The sector is facing the implementation of a lot of new tools, ML-based systems, for example. The sector itself is not familiar with these new technologies and the cybersecurity staff is not familiar with them either; however, unfortunately, the attackers are very familiar with them. A lot of these systems are developed through open source and in an open environment. So, the infrastructure is very well known.

We also are seeing that increase in attack surface in health care and public health. And if you look at things, for example, in telehealth, we see that the care environment now extends from hospital care providers through various networks, various providers all the way through to a person's home. This includes a lot of sensors and laptops and handheld devices, and that all that provides an opportunity for attacks.

We've seen also a slew of supply chain vulnerabilities, anywhere from the delivery systems to manufacturing and so on. We also see a substantial number of attacks against medical record system and medical devices. In the medical record system, of course, is because it's very rich. It provides an opportunity for attackers to make a lot of money, frankly, by getting a hold of these records and threatening to expose them, or just lock them from you. So, we are seeing a lot of the medical record systems being attacked, and the issue of staff training continues to be substantial in health care. Not only the IT folks and cybersecurity in terms of training for them, but the medical staff. Their main focus continues to be, thankfully, patient care, and so they focus on patient care and that sort of makes cybersecurity secondary to them, and that is also an issue. Next slide, please.

So, just a little bit of the stats here, just to give you an idea of how bad this problem is. In 2022 there was 210 entities that worked with the FBI because they reported being victims of ransomware. These are only the folks that work with FBI, the actual number is higher, as there are people that do not report to law enforcement. And also, there was a study done in 2022 that showed that the health care organization with attacks doubled from 2016 to 2021, and we saw 42 million patients being exposed during that time. For us, a lot of you might be familiar because you were involved in helping us deal with. That was the largest attack at least recently, since the largest one was in last year was the CommonSpirit ransomware attack. That attack compromised 623,000 patients, but also disrupted the delivery of care in multiple facilities. For rural hospitals that are operating on really small margins, and today they really don't have the budget or IT staff, sometimes you see people wearing multiple hats and it's where we see they are being targeted increasingly, and they also have a tough time recovering from these attacks. Next slide, please.

So, what motivates people to target health care and public health? The large majority of these attacks are financially motivated. They are cyber criminals, and they do this for money. But we also see state-sponsors that do this to disrupt the national critical functions, and we also see a marriage of convenience between cyber criminals and the state sponsor attackers. Increasingly, you see a lot of that as well. And then we saw a continuous increase in activism, during COVID and post COVID. Those come mostly in terms of a distributed denial of service to disrupt the service. Next slide, please.

So, I don't have to tell you, you already know how complicated and complex the ecosystem of health care and public health is. There are many different pieces and parts and subsectors and segments of this. I won't go through it all, but you know, from hospitals to technology providers, labs, they all create an interdependency where the destruction of labs, for example, has extended to hospitals, for example. Next slide, please.

So, what happened in health care and public health? Ultimately, we talk about patient safety. And our goal, although the financial factors are substantial and important, but for us, for hospitals, and patients, it’s about destruction and delivery of care. You've seen, increasingly, that attacks hit hospital tools and devices that are critical to delivering patient care. And we are currently dealing with an attack in the hospital that delivers radiology services for cancer patients. And that attack actually disrupted the delivery of care for a number of days, 4 days. They are just starting to recover from that, and the attackers know that it by targeting these delivery systems, it’s more likely that the hospitals would pay the ransom. The other issue that is becoming more and more concerning is an attack against one hospital, one that’s care delivery system extends to others, because the patients have to be diverted to other enabling hospitals. A lot of the risk assessments that we do is contextual. So, what that means is that again, when we try to measure the extent of risk that a cyber-attack has caused, we look at it to see what other hazards are happening in the area over there. There is also dealing with forest fires. There is an incident, for example, now in the Caribbean that we are concerned about, where we are really focusing on hospitals. Next slide, please.

So, I'll talk to you a little bit about all the risks or the cyber threats that affect the interfaces. I'd also told you before that the assignment of the Sector Risk Management Agency, or SRMA, who look after this critical infrastructure for health care and public health has a very large database, almost 90% or more owned and operated by private sector through their role of us as the SRMA. A lot of it is about building a collaboration space with our private sector partners, working very closely with them.

Okay, from all-hazards angle, from the SRMA angle, I have some of my colleagues looking at the sector through different lenses. Of course, my lens is cybersecurity. And so, a lot of that work is sector coordination and serving, in terms of day-to-day, as a federal interface and for the prioritization of sector activities. We built a lot of task groups to identify and address, as well as develop the strategies for mitigating cybersecurity risks. Right now, there are 17 joint task groups that are operating the private sector. And there's also 4 or 5 programs that also develop procedures for mitigating cybersecurity risks. That office runs from the OCIO and is under the Sector Risk Management Agency award. And then we also do a lot of threat assessments. We do a lot of intelligence gathering. We work very closely with DHS for it, with NSA, with the FBI, to identify the threat factors to find what is happening in the sector, and then develop mitigation and share that information with our partners. And then also we do a lot of incident management. We monitor major cyber incidents in the sector. Of course, we don't own those the assets. For the most part, we do a lot of risk assessment in terms of what it does in terms of the delivery of care. Very recently, we just developed a risk management product and risk assessment. And we do get involved. We do an assessment of risk, the impact to the sector for the delivery of care, and we support the Nation in the cybersecurity policies. Next slide, please.

So, just to give you a little insight of how we do this work. On the public side, ASPR is the coordinator between sector risk management agencies and the government. And that’s so as to manage the government coordinating council that’s in HHS. All the operating divisions that are the stakeholders are in healthcare and public health. There is a council that also ASPR manages, and there are working groups under these, both GCC and HHS that ASPR manages. And there's a lot of work that happens on the public sector side. On the private side almost the same. There is a council that has been set up with private sector partners, and they elect their own leadership. They have working groups and subtask groups, and so on. And we come together, as this joint task group, I’m the co-lead of the Joint Cyber Working Group along with my partners from FDA and OCIO, and we have folks from the private sector side and the Council. Under that we have a lot of joint task groups that look at all the emerging and ongoing cybersecurity risk and sector risk. Next slide, please.

Again, within this, just inside the GCC, just give you a little view: the cybersecurity working groups work very closely, as I said, with state and local authorities, with the FBI, and the NSC. We do a lot of collaborative work with SRMA. In other sectors, there's a lot of dependencies that we all have to ensure that we share a lot of information. And all this really works ultimately under the leadership of a DHS or CISA, which oversees all the security risk management agencies Next slide, please.

So just a little bit about what the major tasks that are ongoing. Earlier this year, there was a lot of attention from the White House on the role of the Sector Risk Management Agencies and cybersecurity. Health care and public health has been at the top of everyone's attention. So there is a lot of attention from the Secretary and on improving and harmonizing the SRMA functions. So, we are working very closely with the Deputy Secretary's office and with our other partners within HHS, FDA, CMS, etc., to harmonize our activities as the Sector Risk Management Agency.

We are also involved in updating the Health Care Industry Cybersecurity Task Force report. If you remember, I think it was maybe about six years ago, that at the request of Congress, HHS led the joint efforts to develop a Health Care Industry Cybersecurity Task Force report, which provided a blueprint for us to work in terms of just identification services to use identification and mitigation strategies. It's been a while; it's now time to update it. And then there's a lot of work that that's going on to update that plan. We are targeting the end of this year. And as I said this, we have, finally, after a couple of years of effort, we have developed a HPH Sector Cyber Incident Management Plan. It is very much focused on coordination of activities within HHS in response to cyber incidents.

Now, we are working to expand that outside of HHS coordination by working with other agencies that are involved. The NIST Cybersecurity Framework Working Group released an implementation guide sharing very substantial work. It's a very big, detailed document. If you have not seen it, it’s on ASPR’s website. We received a lot of attention from Congress for releasing that. Now we are working this year to incentivize our sectors, to move towards adopting the cybersecurity framework and design and operate their environment accordingly.

This year, Congress passed a law which obligates the reporting of cyber incidents to the Federal Government, and the implementation of that the law has been passed to DHS and CISA, and we are working very closely with them to operationalize that. Also, there is a lot of work that's happening now in terms of development of performance goals for health care and public health. There’s a lot of work now in terms of improving the cybersecurity posture of public health and small, rural health care. We see that they are increasingly targeted, and there are communities that are less abled and resourced, so we work closely with them.

00:32:31.880 --> 00:32:39.409

**Angela Krutsinger:** And Bob, we're right about at time.

00:32:41.060 --> 00:32:44.669

**Bob Bastani:** Thank you. I just have one more slide, I think. We are doing a lot of work with HPP. And I just wanted to bring that up. A lot of you are familiar with some of the work that we are doing with our HPP colleagues, and this is one of them in terms of the cyber-event essential elements of information. If you go to next slide, I’ll wrap it up. We’re also investigating developing incentives for smaller and financially distressed providers to meet minimum cybersecurity standards.

Sorry. I went through a lot of information in a very short amount of time, and my contact information is here. I do want to close my presentation by asking for your help. The Cybersecurity Working Group, the task groups, they all are dependent on people that have assets and knowledge and implicit knowledge of the environment. So, it's an open invitation to join these task groups. Join the work, and if you're interested, send me a quick email. We would love to have you. With that, I'll stop and answer any questions that you might have.

00:34:20.989 --> 00:34:37.440

**Heller, Matt:** Bob, I know there is one question in the chat from Eileen, who asked, “Are some of the attacks fueled by entities who are trying to steal new advances in health care, medicine, etc., especially in facilities that also have large research components?”

00:34:38.110 --> 00:35:08.139

**Bob Bastani:** Oh, absolutely. And we saw a ton of those type of attacks during COVID. As our partners were busy developing therapeutics and vaccines, we saw a lot of attacks for the stealing of intellectual property and that is a huge concern, and we are continuing to see that, of course.

00:35:12.330 --> 00:35:39.629

**Angela Krutsinger:** Great. Well, thank you, Bob, so much for the presentation. And thank you, Eileen, for the question. We'll now pass it over to Rachel Lehman, the acting director of ASPR TRACIE. If there are any other questions for Bob, he did include his contact information in the presentation, or you can always reach out to your field project officer, and we'll pass those questions up. So, I will now turn it over to Rachel.

00:35:40.220 --> 00:43:25.260

**Rachel Lehman:** Thank you, Angela. It is such a pleasure to be on today's call. I'm excited to highlight ASPR TRACIE's cybersecurity resources, as well as some of our new and upcoming products. Next slide.

So, our cybersecurity resources are some of our most popular resources, and I think, after Bob's presentation, it is understandable why that is. In fact, our Cybersecurity Readiness and Response Considerations Document is our most downloaded ASPR TRACIE product. If you're not familiar with the Cybersecurity Readiness and Response Considerations, the origin of the documents was in 2020, when ASPR TRACIE received a technical assistance request from a hospital looking for specific considerations related to the effects of a cyber incident on the health care operational environments, and that impacts the ability to effectively care for patients and maintain business practices and readiness during such events. There are already great resources available that discuss the IT response to a cyber event, so our considerations document focuses on the health care operations and assuring patient care. The document is intended for a large-scale cyber incident, but many of the strategies and principles outlined are relevant to a range of cybersecurity incidents and health care facility types. So, the consideration document is split into three large categories: preparedness and mitigation, response, and recovery. But overall, the document is focused on five key actions for health care facilities: first ensuring consistent surveillance of their systems, being able to identify triggers and go to immediate shutdown in escalation of the issue, communicating to all stakeholders, implementing business continuity processes, and lastly, implementing downtime recovery processes. This document and the accompanying national webinar and speaker series recordings were done in collaboration with Nebraska Medicine and MedStar, who provide extremely valuable real-world examples of their hospitals’ responses to cyber-attacks. The document was originally published in February 2021, and with the help of subject matter experts, we updated the document in October 2022. The update was conducted to provide new case studies and examples and to include updated information and considerations.

In addition to the Cybersecurity Readiness and Response Considerations Document, we have a Healthcare Cybersecurity Resource page and a Cybersecurity Topic Collection on the great products that CIP and the HPH sector and cybersecurity working group products, can be found in the Cybersecurity Topic Collection. Our second issue of the Exchange, also focused on cybersecurity and cyber hygiene. And then, lastly, we have a cybersecurity section on our select TA response web page. There are some incredibly useful TA responses in that section. So, I highly recommend reviewing that webpage when you have the time. Next slide.

I'm looking forward to our new and upcoming products. Since we last updated this group in March, we have, really, several new resources that we are very excited about. In April, we had a round table featuring speakers representing a wide range of stakeholders and jurisdiction types sharing their perspectives on how they integrated lessons learned during COVID-19 in recent incidents and into current and future responses. Some of the topics covered in the roundtable include channels used for outreach and continued engagement, strategies for reaching different community and control groups, tracking and countering rumors, and working with partners to create complementary messaging. As we did for the other provider supplier types that comply with the CMS EP rule, we created a facility specific requirement overview document or crosswalk for rural emergency hospitals, which, as of January first, are a new provider type.

Last week, we released our seventeenth issue of The Exchange. In this issue you can find experiences and lessons learned from healthcare facilities and systems that endured water and other utility outages because of severe weather. Specifically, you can read about the effects of the Jackson, Mississippi water crisis on a health care system, how facilities in Texas incorporated lessons learned from the 2021 Winter Storm Erie, which led to power and water outages at several hospitals in Texas. The significant impacts that Hurricane Ian had on hospitals in Southwest Florida, and how the Northwest Healthcare Response Network, with hospitals across Seattle and beyond, managed a severe heat event in 2022. We've already received a lot of really great feedback on Issue 17. So, if you have not had the chance to read it, I highly recommend you do so.

Our new Mass Casualty Hospital Capacity Expansion Toolkit is a concise, scalable search response templates, which can be a helpful with reference to the hospital personnel tasks of expanding care capacity in the first hours of a mass casualty incident and can minimize the ad hoc and potentially conflicting decisions about prioritization of space and strategies.

We released a Medical Countermeasures Commercialization Resource Page, which provided resources for stakeholders for interest in the commercialization of vaccines, therapeutics, and other products developed with the support of the U.S. government, and later transitioned to commercial channels.

Then, in collaboration with ASPR leaders and in honor of pride month, we release the LGBTQI+ Community and Disaster Preparedness and Response Topic Collection. This is our sixteenth topic collection, and it provides resources for LGBTQI+ individuals, tools for planning, resources for emergency planners and health care providers, resources specific to behavioral health, and resources that provide lessons learned from the COVID-19 pandemic, mpox, mass casualty incidents, and natural disasters. The information and resources include in this topic collection can help emergency planners and health care providers create a more inclusive environments after a disaster occurs.

We continue to release Utility Disruption Speaker Series recordings, and we recently comprehensively updated our Risk Communications, Social Media and Emergency Response, and Utility Failures Topic Collections. To be noted, our Risk Communications and Social Media and Emergency Response Topic Collections, both now feature our misinformation and disinformation session. Next slide.

And I want to flag some of our upcoming products, as well. As most of you know, the round table will be held in April. We are putting together a Lessons Learned in Health Care Communications document. It will be an “experience from the field” article. Of particular note, we are updating the EMS Infectious Disease Playbook. The original playbook was developed in 2017, and we've been working with numerous subject matter experts to incorporate new considerations. The updated playbook will be available later this month. You can expect the updated health care provider shortages, resources and strategies for the demand documents, and the health care facility on boarding checklists later this summer, as well. Keep an eye for the updated topic collections you see on the slide. We'll be releasing those throughout the summer and the fall. Finally, if you're attending the Joint Commission Emergency Management Conference later this month, please check out the 2 sessions from our senior editor, Dr. John Hick, on the DASH tool and workplace violence. Next slide.

Thank you all for listening and thank you to the Office of Health Care Readiness for having ASPR TRACIE on today's webinar, and I'm happy to take any questions if there are any.

Okay, the sound of silence. Please do not hesitate to contact ASPR TRACIE if you do come up with any questions, and with that I will pass it back to you, Angela. Thank you.

00:43:25.830 --> 00:44:00.179

**Angela Krutsinger**: Thanks so much, Rachel, and thanks for the great presentation and to the entire ASPR TRACIE team for putting together such a comprehensive and relevant materials. So now we'll have the general Q&A. We have a few minutes before the top of the hour, so we would like to open the line for any other questions, for either the presenters, while we have them, or for ASPR in general.

00:44:22.710 --> 00:44:31.710

**Heller, Matt:** Angela, I see a couple of questions coming into the chat. The first one is from James Moss, who asked, “When should we expect our final BP5 budgets?”

00:44:31.760 --> 00:44:59.010

**Angela Krutsinger:** Yeah, we still have not received those. As soon as we do, we will make sure that they get sent out. We have been reviewing the applications that were submitted in Grant Solutions. And we will finish those reviews this week so that the notices of award will go out on schedule by July 1st. As soon as we do receive the HPP BP5 final budget numbers, we will definitely send a notice out to everybody.

00:45:01.100 --> 00:45:49.899

**David Csernak:** And it looks like there's also a little follow up there asking, “Is there any update on the timing of the HPP NOA?” And I mean, I can answer that one really quick. So, the NOAs are still on track to be issued by July 1st, which they traditionally are, you may see them a day or two early (by the end of June) populate in Grant Solutions, but they are set to be released on July 1. So, you know, the funding is there and ready to be dispersed. The NOAs are on track to be released. But, like, Angela said, we don't have the final numbers for BP5 to be published yet, but that doesn't mean that the funding is not there, and the NOAs won't be provided on July one.

00:45:51.540 --> 00:46:54.439

**Angela Krutsinger:** Also. Matt, can we go ahead and put the MRSE slide back up again that we had promised to circle back to? Thank you. Okay also, there was a question about the PERFORMS application module stating that it's open until the 31st of December. Yes, that's just a placeholder. We expect the numbers will be before the 31st of December, of course. But we had been asking them to keep it open, you know, a couple of weeks at time, and at this point we just asked them to push it back so we did not have to keep doing that because we had anticipated, of course, that those numbers would have been received by the 16th, which is this Friday, but we have not seen them yet. So that's just a number that was pulled out to do that. Okay? And I think we've already answered the NOA question.

00:46:55.470 --> 00:47:03.620

**Heller, Matt:** There was one question from Edwin who asked, “Can surge estimator tool be explained again?” and I believe that relates to the MRSE.

00:47:03.830 --> 00:49:07.590

**David Csernak:** Absolutely. So, we can explain that one for you again. So, in the current the FOA, there was a requirement for the Surge Estimator Tool to be completed by health care coalitions every other year. So those years being FY19/BP1, FY21/BP3, and then FY23/BP5. Thanks to our mutual friend, COVID, the BP3 requirement to complete the Surge Estimator Tool was waived, so coalitions completed it in BP1, and then it was waved for BP3. As we started looking at developing a continuation application guidance for BP5, we realized that a lot of coalitions were actually conducting a surge estimator survey to some varying degree across their coalition members as part of the MRSE planning process. So, as they were beginning to develop their exercise scenarios and their exercise plans to complete the MRSE requirement, they were actually looking at very similar types of surge information and surge estimation totals across their coalitions to help complete that exercise. So, in order to help reduce burden and build on something that they were actually using in a more functional and operational way, we decided to basically integrate the Surge Estimator Tool into the MRSE toolkit to assist coalitions in collecting that data as part of the exercise. So, rather than it being a separate standalone requirement, it's now just integrated into the MRSE itself. So, as the coalitions look at the upgraded tool, once we publish out the upgraded tool for BP5, they'll see the Surge Estimator Tool piece built right into that tool, and it should assist them with better preparedness and better planning for conducting the MRSE in BP5 and eliminate the need for a second standalone requirement. I hope that answers that question for you.

00:49:11.550 --> 00:50:35.779

**Angela Krutsinger:** And then also, we had a question asking, “Why was the feedback deadline was extended on the pre-decisional draft? Are you overwhelmed with suggestions? You're simply hoping for more? Are any significant changes in the works?” Well, those are 3 questions. So, I'll just go ahead and go through those quickly. The deadline was extended for several reasons, but mainly to continue to get feedback. We have received thousands of comments and different suggestions for that and are working on compiling those. But by popular request, we did extend the deadline for that additional week, and of course, there will probably be some significant changes in the works for that. We won't know what those are until we see the final draft. And of course, as soon as there is a final draft, we will make sure to share that with everybody. I do not see any other questions in the chat. I see lots of applause, for it would be helpful to receive the in NOA before July 1, and of course GMS. Will do their best to try to do that. Right now, that is the schedule, is it, you know, no later than July 1, to have those up.

00:50:36.600 --> 00:51:04.949

**David Csernak:** Keeping in mind, too, the numbers that are going to be released in the NOA are, for now at least, the same budget numbers that you utilized during your budgeting and application process. So even if the NOA is issued before July 1, it doesn't take effect, and the funding doesn't become available until July 1. So, for now, the information that you have is the most accurate and most current information to utilize for any of your contracting and budgeting needs. Once information is received back down from the ASPR, if budget numbers are changed, then that update will be made as well. But the information that everyone currently has is the most current and accurate budget information.

00:51:28.450 --> 00:51:44.180

**Angela Krutsinger:** I am not seeing any more hands raised.

00:51:48.730 --> 00:52:02.530

**David Csernak:** I’m seeing some comments about some contracting delays, but I don't know what else to offer as far as advice at this point.

00:52:03.940 --> 00:53:41.330

**Angela Krutsinger:** Okay. Oh, there is just one more here, “When responding to conditions of award or needs more information, the COAs or NMIs, would it be due 30 days after receiving the notice of award, or the additional funding?” Usually, it is written in the notice of award that is within 30 days after receiving the notice of award.

Okay? So that answers all the questions that we've had so far. So then, thank you all for your questions, and I'll ask to go to the closing remarks slide.

Thank you to all of our presenters for their time today and to all of you for your active participation in today’s meeting. As a reminder, we invite you to share any stories regarding how you or HCC members are using ASPR funding to make a positive impact on their communities. If you have a story to share, please fill out our Stories From the Field Submission Form or reach out to your field project officer for more information. A member of our team will drop the Story From the Field Submission Form link in the chat for easy reference. We look forward to hearing about the great work that you're doing and thank you again for attending today. Have a great day, everyone!