FEMA Administrator Deanne Criswell's Remarks to the National Emergency Management Association

Release Date: Oct 4, 2023

It is great to be with all of you here in Memphis.

The deadliest fire in modern history on Maui. A bi-coastal kick-off to the hurricane season with three Category 4 storms, Hilary, Idalia, and Lee. That was our reality only weeks ago.

We planned, we prepared, we responded and began the recovery efforts. That's what we do.

To those involved in the response and recovery on Maui and in the states and Tribes affected by the hurricanes, let me thank you for your heroic efforts on behalf of survivors, their loved ones, and tragically, those we lost.

I saw your work in action firsthand. I witnessed your nimbleness, your tireless advocacy, and your compassion and caring for those who lost homes, businesses, and loved ones.

FEMA is always proud to work with and beside you in the aftermath of these events.

It is true—extreme weather events are on the rise. And as I have said before, the changing climate is making them worse, less predictable, and more frequent.

But the response and recovery to natural hazards are already ingrained in us and in our playbooks. We know how to get ready for them—even though the response and recoveries are becoming far more complex.

And, we continue to learn and improve through all phases of these disasters, at all levels of government, and with our vast network of partners in the public and

private sectors.

So, that said, what keeps me up at night? Where do I think we need a stronger preparedness focus? It is not the next storm, fire, earthquake, flood, or tornado. Although certainly, those risks are worrisome.

What keeps me up at night is the looming danger presented by nation-state threats to our homeland.

As state emergency managers, you know all about these threats. You are seeing them more often back home. You even train for them.

However, we are also facing increasing priorities, the pace of natural disasters, and tight budgets, and sometimes cybersecurity threats aren't top of mind or on the first pages of your response manuals.

They should be. That is what I want to talk to you about today:

- What a nation-state attack might look like.
- Why you should care.
- How FEMA views consequence management and lessons we can share with you.
- And finally, the need to balance our approach to climate-driven disasters and nation-state threats to foster a ready nation.

Let me set the stage.

After the East Palestine train derailment, the EPA was there, the National Transportation Safety Board (NTSB) was there, CDC was there, FEMA was there, and you were there. So were Pro-Russians actors.

Media reported that anonymous pro-Russian actors used X, formerly known as Twitter, and TikTok to spread anti-American propaganda. These false stories about the chemical spill created fear, anger, and confusion in the community.

In the aftermath of the Maui fires, we were there, you were there. So were Pro-China actors. The contested information they spread impeded our ability to register people for disaster aid.

This ‘spamoflauge’ paraded as information, disseminated conspiracy theories about the cause of the fire and the government’s role. These incidents underscore why we must pay attention to identifying and countering these influence campaigns against us.

Let’s face it, disasters are fertile ground for the spread of false information. When our eyes are on helping survivors, our adversaries are stoking our most triggering emotions.

By some estimates, these examples represent only a small fraction of the problem.

Microsoft warned us recently of a new Chinese cyber threat. Called the “Volt Typhoon.” These stealth attacks have the capability to seriously compromise critical infrastructure and are a challenge to hunt.

Earlier in the year, Chinese hackers exploited a vulnerability in the encryption that protects a cloud service, breaking into the networks of hundreds of private sector organizations and reading sensitive email traffic.

A more visible example was the Chinese spy balloon hovering over U.S. airspace for days. The decision of where and when it might land or be shot down involved our states, locals, and even Tribal Nations. It captivated the Nation’s attention.

I doubt any of you had a tab in your playbooks for “spy balloons.” However, it was a perfect example of how these threats do not respect our political subdivisions, nor do they respect our decentralized response authorities.

The most recent Intelligence Community’s threat assessment warns us that China will not just be hacking and stealing data in the future but is developing the ability to use the ‘cyberverse’ to aggressively disrupt and even destroy our critical infrastructure.

Such a move could endanger oil and gas pipelines, even rail systems. China may feel emboldened and capable of creating societal panic in our country.

This is just one reason why we must demonstrate our collective cyber resilience. Let’s face it, our critical infrastructure systems are so interconnected, a formidable cyber adversary like China might find it easy to exploit their vulnerabilities.

And we need to worry about other foreign actors and possible chemical, biological, radiological, and yes, even nuclear threats.

According to the Homeland Threat Assessment published last month, CBRN threats to the Homeland will likely continue because of foreign, political, and military developments and the global proliferation of laboratories working with dangerous biological pathogens.

What's clear in this latest assessment, is that the challenges we face here at home are more diverse and complex than we've ever faced before.

While deliberate use of such threats against the Homeland will likely be limited, we have heard Russia's public allusions to using nuclear weapons as part of its invasion of Ukraine.

Such statements demonstrate that international actors still consider nuclear threats as viable tools of statecraft.

Meanwhile, the growing nexus between AI and scientific research—especially in biotech—is increasing the risk to public health.

It's even caught the attention of Members of Congress.

During a Judiciary Committee Hearing this summer, senators on both sides of the aisle raised concerns about how AI tools could increase the risk of deliberate or incidental creation of novel chemical compounds that could be used to harm us.

While CBRN threats occurring abroad may not reach the Homeland, they have the potential to disrupt regional and global commerce, harming US economic interests.

When we talk about what a nation-state attack might look like, we realize it could develop slowly at nuisance-level activity. These activities would build until they eventually become disruptive, as we saw with the Colonial Pipeline attack.

If that doesn't stress our emergency management community, more severe, destructive attacks certainly will. If we are not prepared, these attacks will quickly become overwhelming for us and our communities

Our adversaries understand how to manipulate information to spread fear, anger, confusion, and distrust in the Government. In some cases, this is their clear goal.

They understand how to use social media to create chaos. They have demonstrated a willingness to use cyber tools to hack and disrupt on a national scale.

The scenario I am describing may not be easily recognized. Our adversaries won't be using vehicle-borne IEDs or flying aircrafts into buildings like the terrorist attacks on 9/11.

The Office of the Director of National Intelligence recently released a new Annual Threat Assessment, which I encourage you to read if you haven't already.

According to this report, our adversaries are far more likely to hijack our power grids, our telecom infrastructure, or our financial institutions, and disrupt our military's ability to mobilize.

It may start in one state and spread to others.

It may look like a simple power blackout in the Midwest until the map of our great nation is lit up with incidents of all types. Social media will be buzzing with conflicting reports to steer us into chaos.

This is what a campaign might look like. And it's a challenge that will require a whole-of-society effort to address.

Consider this. The Port of Los Angeles handles $250 billion in cargo, and according to Gene Seroka, the executive director of the Port, it now faces 40 million cyber-attacks a month.

He attributes the attacks—from ransom and malware to spear phishing and credential harvesting—to pro-Russian actors and their desire to disrupt our economy.

But it's not just big commercial hubs that are feeling the impact. I met with North Dakota Governor Burgum a few years ago at a Western Governors Association Conference.

And you know what he told me? In 2018, cyber actors associated with North Korea infected one-third of North Dakota schools with malware. This was a major threat across the state.

Thankfully, the threat was contained, but clearly this isn't just about big, flashy targets.

From Wall Street to our busy seaports, to rural hospitals, Tribal Nations, and communication systems, we must face this new reality: Clandestine attacks are becoming more brazen with consequences that will be catastrophic.

That is why it matters to you. And that is why we must turn our immediate attention to these threats and treat them just like an impending natural disaster. We must prepare at all levels to mitigate and develop easily executed solutions.

In short, we must do this together. We must break down our silos and cultivate new partnerships between us and with our defense and intelligence agencies.

We need to leverage the collaborations CISA is building and the expertise across the entire Federal Family.

We need to combine that with alliances with private sector partners who have a wealth of knowledge, technological solutions, as well as wide-ranging responsibilities in the various critical infrastructure sectors.

From there we can use best practices to meet these growing and sophisticated threats.

We can take lessons from COVID-19 to help in our strategic approach.

During the pandemic, we invigorated dormant framework agreements to overcome supply chain issues and enable the public health and medical community to meet the moment.

We used the Defense Production Act in a new way to mobilize our nation's capacity.

Imagine that happening in a geopolitical conflict with multiple attacks on our critical infrastructure and the possibility that DOD support might not be available.

We have to make sure our states continue to support one another and can share resources effectively. It is a vital part of our national resilience.

However, we also need to be more aware of China's intentions, and what it is capable of, as we plan. In an April 2020 speech, China's President made it clear that he wants to exert more control over the global supply chain.

Such an approach could give China the ability to threaten or cut off foreign countries from key resources during crises.

Likewise, we need to think through how to use Command and Control (C2) more effectively when all of our authorities, not just the Stafford Act, are needed at the same time.

Collectively, we must evolve. It starts with us and a shift in our mindset as emergency managers. It involves pivoting away from a terrorism-centric view of homeland security and realizing that homeland security is national security.

Yes, there is a balance that must be achieved in how we use limited funding to address both climate change and nation-state adversaries.

Across our federal family, we must leverage our strengths. We need to find and fill gaps because response cannot solely rest on the shoulders of the DOD and Defense Support of Civil Authorities. And we must collaborate before an incident.

I have been pushing my staff to work with the DHS Intelligence Enterprise and the Intelligence Community to get sensitive intelligence to a place where we can more easily share it across agencies, and act on it in a timely manner.

While we were successful at intelligence sharing at the beginning of the Russia/Ukraine conflict and the Chinese high altitude balloon incident, we have more to do. We have to be able to share intelligence more rapidly.

At the federal level, we're making our voices heard. We're getting into rooms where the decisions are being made. We're pulling up chairs to the tables where intelligence is being shared.

We are communicating what our information requirements are. And we are advocating to get tearlines on intelligence so we can share and use it more

efficiently.

We're bringing people with us too. Earlier this year the ODNI brought senior level decision makers from across the intelligence community together for a classified two-day table-top exercise.

FEMA was involved in the development of the exercise and we realized that having state participation would be critical for it to be successful.

Our other federal partners agree, and we were able to get Mr. Shawn Talmadge from the Commonwealth of Virginia cleared to participate. Shawn, if you're here, thanks for supporting that event.

We will continue to push for expanding the footprint of our state-level partners in future events like these. Because information sharing is critical for responding to these types of threats.

I need all of you to do the same.

I need you to go back to your state and local governments and advocate for getting into these rooms and breaking down barriers to information.

Right now, the Department of Homeland Security is pulling disparate information from across the Federal Family—signal intelligence from NSA, briefs from human sources from the CIA—and fusing it into usable information for emergency managers.

We use this information at FEMA to inform our day-to-day activities. But this information isn't just for us—your fusion centers and intelligence partners can access it too.

YOU need to make sure you're getting that information, hearing that information, and using it to your advantage as you develop planning strategies to prepare and mitigate these threats.

So, as we work at the federal level to get you the information you need for these looming threats, here is what you can do for us:

Tell us what you need to better prepare.

Help us modernize our collective information-sharing environment so we avoid being overwhelmed by escalating activity.

Be proactive in your planning to incorporate these threats and their required partnerships.

Look for, take, or even create new trainings for your personnel and jurisdictions, and share them.

Establish your own public/private/military relationships and frameworks for collaboration before an event.

I cannot stress enough the value of information sharing and partnerships.

We have seen our response to natural disasters improve steadily over the years because we have crossed state lines and other boundaries to communicate and cooperate ahead of time.

Adding new threats to the mix means streamlining and expediting information sharing to make our responses seamless and timely. It also means developing a coordinated approach to combating contested information.

I am the first to admit that this is a tough environment to balance priorities in. Budgets are tight everywhere. Together we must strike a consensus on how we manage climate-driven disasters and nation-state adversaries simultaneously.

Just as we see our disaster pace accelerating, so is our risk rising of a cyber-attack that could bring down our critical systems.

We will not have the luxury of watching it approach through satellite imagery. It will lurk just outside the confines of our detection, just under our radar. In other words, we need to focus on planning, because in some cases it may be too late to prevent.

We need to realize that while we are responding to natural disasters, we may unwittingly leave an opening for those who want to disrupt our way of life through information or cyber activity.

For us at FEMA it's meant changing the way we view consequence management when it comes to cybersecurity threats.

Take a recent cyber-security threat stemming from Russia's war in Ukraine as an example. We approached that situation far differently than we approach severe weather events.

We worked with CISA to establish unified coordination and led the consequence management. We had to change our thinking about how to deal with that event.

We had to think in terms of timelines because, unlike a hurricane, we couldn't see its trajectory.

This wasn't a flood, a tornado, or wildfire. There was no clear indication of when response would end, and recovery could begin.

We're not the experts in ending cyber-attacks.

But we *are* the experts in dealing with the fall out. So, we got to work thinking about the cascading impacts.

We started thinking about the contested information environment. We shifted from a preparedness mindset to a planning mindset.

It's something you need to start thinking about on the state, local, and tribal levels too.

What does consequence management for these kinds of threats look like for you and your community?

I can't stress this enough.

Because this is not the stuff of Hollywood. We are gathering more and more evidence that our adversaries are doing more than testing the waters. They are active in this environment, and they are threatening.

As emergency managers, we need to be ever vigilant. I ask you to apply the same principles to these threats as you do to natural disasters. Help your communities build resilience. Leverage all partners. Prepare.

We can no longer put this kind of preparedness on the back burner. It is time to update our playbooks and balance our priorities to make our nation safer and more secure.

Part of developing a resilient nation includes our ability to develop strategies to mitigate threats before they happen. We demonstrate our resilience to those who seek to harm us, and our way of life, by planning and working together,

I look forward to our continued partnership in this ever-evolving landscape. And I thank you for your dedication to serving your communities in these challenging times.

Thank you and enjoy the conference.