Remarks by Administrator Thomas D'Agostino, National Nuclear Security Administration, on NRC International Regulators Conference on Nuclear Security

Release Date:
December 05, 2012

Good afternoon. I want to express my appreciation to the Nuclear Regulatory Commission for the opportunity to talk with you all today. I am delighted to see colleagues from 39 countries around the world representing the nuclear security spectrum here at this conference. The NRC has done an outstanding job of bringing the international community together to talk about the importance of nuclear security and build bridges with counterpart regulatory entities with responsibility for protecting nuclear and radioactive materials.

As the Administrator of the National Nuclear Security Administration, I have a special view of nuclear security, security culture and executive leadership. It is no coincidence this speech takes place in advance of the panel session on responses to nuclear security incidents.

As many of you know, in the early morning hours of July 28th of this year, three individuals trespassed onto the Y-12 National Security Complex and defaced a building where the United States stores highly enriched uranium. While their actions were wholly unacceptable, the intruders who cut through fences never gained access into the facility or came close to any material. Our guard force was slow to respond, but the individuals were interdicted and arrested. As a result, we have learned a lot about our organization, the assumptions we had made, and how we communicate.

The incident at Y-12 was a completely unacceptable breach of security and an important wake up call for our entire complex. The security of our nation's nuclear material is our most important responsibility, and we have no tolerance for federal or contractor personnel who cannot or will not do their jobs. In response to the incident, we have taken strong and decisive action to fix the issues that led to the incident at Y-12.

We took steps that led to the removal of the contractor responsible for the guard force at the facility, we have removed the top leadership at the site, and the officers associated with the

incident were fired, demoted or suspended without pay. Additionally, federal officials with security oversight responsibilities no longer hold these jobs and no longer have anything to do with nuclear security. We also have been working to make the structural and cultural changes required to ensure the security of this facility and throughout our entire complex.

While we're confident that these aggressive actions have enhanced security at Y-12, we will leave no stone unturned to find out what went wrong and will take any step necessary to ensure security at this site and across our enterprise.

There have been a number of reviews that we have been conducting to look at exactly what went wrong. One of the reviews that I directed focused on the NNSA security organization at the Headquarters and its relationship to the field. In that review I asked independent experts to examine the organizational construct and dynamics of our security organization and to provide me with an unbiased evaluation. That review included non-attribution interviews of all layers of the security organization allowing for free flowing, candid information exchange and resulted in the identification of some key concepts for lessons learned.

Some of what I learned I want to share with you today, because it's not necessarily unique to Y-12, NNSA, or the United States. Indeed the lessons apply much more broadly as well to every facet of nuclear industry, ranging from nuclear safety, to project management, to operations.

Before I get to the lessons, one piece of advice I can share is that if you ever have a crisis event, whether in security or any other area, find someone independent who knows your organization and can provide a completely unbiased assessment of ground truth. U.S. Air Force Brigadier General Sandy Finan was on assignment to NNSA already, but as a former Air Force Inspector General, I asked her to step in and lead a review into how we got to this point. What she found has been tremendously valuable. She is tough, independent, and unafraid to tell me exactly where things are good and where things are bad.

There are many lessons that we have learned from our security event from this summer. I want to focus our discussion to high level "take-aways" that you may find useful. You may be looking for me to tell you about a unique and interesting revelation or a special insight that you had not thought about as it relates to our experience. I am afraid that you will be disappointed. What we will discuss are the basics, the fundamentals. But because they are fundamental, it is worth repeating again and again.

The first lesson is to make no assumptions. When General Finan briefed me on her initial findings, one of the most important things I was reminded of was this point: to never assume things are as they seem. This not only applies to me as a leader of a large organization, but also to every individual within my organization. You cannot just assume that what seems real is true, and that after you check that it is true, that it remains static or does not change. The security of our enterprise is constantly changing. It changes because equipment gets old and starts to fail. It changes because people are involved and people make mistakes, and it changes because the threat is always adapting and looking for ways to get in. My experience is from the Submarine Force. In the Submarine Force, we work very hard to remove assumptions and doubt from everything we do. We do this for obvious reasons. Captain Chuck Ellis, my Commanding Officer of the USS Skipjack reminded me of this. He said that at the most basic level, the water is always trying to get in the submarine and my job was to work hard at keeping the water out. He also reminded me that while I am asleep, the water is still trying to get in. So we had to be diligent, constantly asking ourselves if what we are seeing is

true, never assuming that we have things completely figured out. Keep digging, keep poking, keep checking. Never lose curiosity in any level of detail; never think your job is complete. And once you think things have been settled, once you feel like you know the honest ground truth, start all over again. By the time you circle back to where you started from, you'll see things you missed the first time around.

In the Y-12 event we assumed we had complete insight into the security conditions at our sites. We had independent assessment teams checking all of our sites. They performed very thorough inspections to include force-on-force exercises and they wrote reports with summary statements saying that security was "fully effective". And I have no doubt that they were fully effective during the inspection period. However, do yourself a favor. Do not rely on the Executive Summary of a report or a one hour brief on the results of the report. These types of summaries are by their very nature just that: a high level overview of how things appear to be at a particular point in time. Do yourself a favor; do not rely exclusively on independent inspections. Most sites do well on these inspections because they scheduled, prepared and ready to go. It's what happens between the inspections that counts! I assumed that all of our status reports, independent inspections, red teams, and briefs gave me the full picture. They did not.

The second key point here is related to the first, and that is to develop a questioning attitude and get into the details. A strong organization — one committed to continuous improvement — needs to develop a workforce that promotes a degree of skepticism, a questioning attitude and a desire to get into the details. There are some that would say that this questioning attitude may indicate that you do not trust the people that work for you. These people would say that if you question someone about what they have said then you are sending the signal that you do not trust them, that they do not know better, that you want to micro-manage their work. Nothing could be further from the truth! Nothing could be further from the truth!

Asking for details about a situation, a program or an event sends the exact opposite message. It tells that individual and others that you think their work is important. And because of that, you want to take the time to understand their work. It also gives them an opportunity to show you how much they know. It has the added benefit of your being able to find areas where additional attention may be needed. And if during your session of questioning, your instincts tell you that there are issues that may require further investigation, then trust your instincts. This may be best seen by an experience that I had in reviewing one of our construction projects, what we call a quarterly project review. Up on the video monitor was the project director who was going through his project. He was explaining the project status, the milestones and his plan for delivering the project on time and on budget. When I asked about the project risks I was told not to worry, that there are no problems now: that there are no risks to project success. That sent off alarm bells in my head. Every project has risks. The project director was supposed to be asking and answering the same question that I had been asking. I needed someone who felt their job was not to defend the project at all costs, but to deliver the project through hard work on revealing the actual situation on the ground. Remember, the higher up you are in your organizations the more reluctant people are to tell you about problems. This type of thinking must stop. So develop a questioning attitude, get into the details. The independent inspection report summaries gave me the impression that we were on top of security and doing fine. However, within the many hundreds of pages of the report, buried in the depths and into the details of the report, there were indicators that we had more work to do. On this point I am reminded of an Admiral Rickover quote: "The devil is in the details, but so is salvation." I want to encourage you to dig into the details, for only in those details will you find your problems — your devils that will eventually get your project. But if you

get to these devils early on, you will have time to address them, and the chances of success will improve dramatically.

The final lesson the event made clear is the importance of communication. Open communication is absolutely critical. If we have an organization that does not want to hear about problems, then that is exactly what you will get — problems! Typically in reviews of projects, or security, or operations, a nomenclature is used to summarize how things are going. It is called a stoplight chart. Red if things are going poorly, yellow as warning indicator, and green to indicate there are no problems. If we, as leaders, focus on making "everything green," we will get what we ask for — "everything green." But happy days will not last. Time and again when we look at problems with our construction projects, particularly the ones that do not do well, we find that there was reluctance to bring up bad news. This is not unusual. All of us want to be known as problem-solvers. We want to fix the problem so we can tell our boss that things are OK. We have to change the mindset of our managers. If we see a problem and do not communicate that problem to the right people who can address it, then we have failed as an organization. Even if you manage to keep your organization curious and vigilant, it means nothing if there isn't an environment where people are able to talk openly about the things they see. Everyone in an organization is part of the mission. For continuous improvement, we need to use the collective brainpower that makes up our organizations.

As a leader, I am well aware that there is a tendency not to bring me bad news or even to express opinions that disagree with my own. It's hard to see what's really going on because nobody wants to tell you – they want you to see what makes them (and you) look best. This leads sometimes to the development of a "clay layer" of middle management where bad news is filtered out and unable to pass through. Where only the positive information comes through, providing a false sense of security.

Leadership needs to ensure that their entire organization understands that we want to hear about problems. Not only do we want to hear about problems, but everyone needs to also understand that it is their obligation to bring problems to our attention. With this openness there also needs to be reassurance that leadership will not "shoot the messenger." You have an obligation to the security of your nation and to the security of every other nation in this room to incentivize honesty and openness.

We will continue to share lessons learned that come from this event and others with our colleagues around the world who are responsible for implementing national and international nuclear security programs. We have an obligation to do so. And all of us in this room have an obligation to learn from each other, get stronger and ensure the safety and security of people around the globe.

Remember:

- When your managers tell you that they have no problem, you should perk up and start asking questions.
- When everything is green, you should be worried.
- When you sense that your team appears to be defending their projects from your questions, you need to re-calibrate them.
- When someone tells you not to worry, you should worry.
- When someone tells you that the level of detail you are asking about is too much for someone in your position, you dig deeper.

There is a phrase we use in this country when something is very clear and easy to understand. We typically say “This is not rocket science!” That phrase holds true right now. Everything I have said is “not rocket science!” You have all heard of these types of things before. Everyone in this room has a problem they don’t know about yet.

1. Make no assumptions,
2. Develop a questioning attitude and pay attention to the details, and
3. Embrace full and open communications — then you will find it.

Only after you have done these things will you have rooted out the problems in your organization. Not just security problems, but safety, financial, management and personnel problems.

Thank you.