**15226, Ralph Corbitt – Due March 22**

Good Afternoon Ladies and Gentlemen,

In a recent report, Dr. Elizabeth Sherwood-Randall, Deputy Secretary of Energy said, “Across the Department of energy we rely on digital technologies to gather, share, store, and use information that protects national security, enables ground breaking research, and increases the efficiency of our operations.” Our increasing reliance on technology puts our entire operation at risk due to our vulnerability to the cyberattack of our technology. It is because of that vulnerability that each one of us in the Department of Energy must take a stand for our cyber security.

We have a new strategy to protect us from cyberattack, outlined by CIO Michael Johnson. He reminds us that it will require a collaboration across departmental lines and over the entire ladder of responsibilities to implement the necessary cyber security. It will require not only increasing current security measures, but implementing new and innovative practices. Because we have had past success in this area, we know how to continue evolving to create new cyber protections as cyberattacks change and as technology changes.

The most important aspect of this new strategy is that we collaborate and leverage the diverse perspectives and experience from throughout the DOE. According to this recent report, there are three important principles and they are that information is a departmental asset, effective information sharing and safeguarding requires a distributed and standards based risk management approach and that above all, the public trust is critical to our success.

The DOE will apply these principles to four strategic goals. We will share enterprise information more effectively with authorized users. We will do everything possible to safeguard information against cyber threats. We will seek out and win the best cyber talent. And we will mature and strengthen the DOE’s cyber posture. Our success hinges on our ability to collaborate and innovate. We can’t stick to the old methods of protecting and safeguarding our important information when cyberattacks change continuously.

Cyber technology changes at the speed of light and we must not only keep pace with it, we must stay ahead of the game on this. We must learn to collaborate with other departments within the DOE, with other government agencies, with the private sector, and with other countries so that this security can be maintained and improved as technology improves.

As we grow and improve our methods we must learn to adopt best practices in regards to cybersecurity. Among these best practices we must have a national information exchange model, we must have a cybersecurity information exchange framework. We must have a structured threat information expression. We must have trusted automated exchange indicator information and we must have a systems engineering body of knowledge. All of these working together will greatly aid in our continued success. While implementing these new safeguards we must be sure to continue to strengthen privacy and civil liberties protections to our information sharing operations. It does us no good if we sacrifice the civil liberties our country is founded upon in order to protect the information that we share.

As we move forward with our continually improving methods we must know that attacks to our security will continue and improve. As they do we must continue to improve our sharing practices, just as we must also improve our detection capabilities. We must be certain to be just as well equipped as the cyber bandits we fight against. We can spare no reasonable method or expense in this. The threat is so much greater in today’s world than it was a generation ago. We have the talent and resources so we must put them to the most efficient and productive use, while we continue to develop future talent and resources.

As we fight to improve our safeguards we must also develop the tools and processes to make notification of cybersecurity threats made known more quickly and accurately. Along with faster notification time, we will need faster analysis and response time, and when a threat is found and stopped we need to also create and put into place a response and recovery process to contain and stop any cyber threats. We have learned from experience that the sooner we can process information that we learn, the sooner we can overcome the threat.

In order to accomplish these bold goals we must recruit a robust cyber workforce. They must have multi-disciplinary talents. This recruitment can be from other companies and organizations, as well as from universities. Recruitment will include enticements such as internships, cyber-based completions, student loan repayment programs and executive loan programs. In addition to recruiting new workers we must continue to develop our talent from within so that our current workforce stays up to date on their skills. But, then, that is normal and expected in the field of technology. Then both our current workforce and our newly hired workforce must learn to work together to combine the experience of the old with the newer training of the young. This combination will be unbeatable against any serious threat to our security.

In order that we might continue to develop our talent both from the inside and from the outside we will use cross cutting initiatives to leverage science, technology, and engineering capabilities to provide security from all sides of this issue. In order to do this we will work with other agencies, industry, National laboratories as well as academia. There are strong talents within each of these disciplines that will aid in the battle for cyber protection. Not everyone will do the same job. Just like in the military, not everyone mans the machine gun. Some people must feed the person manning the gun with a continuous supply of ammunition. Some must build the weapon. Some must transport the vehicle since it can’t operate on its own.

So that we may continue to improve we must evolve how we engage with federal, state, local, tribal and territorial governments, the private sector and academic institutions. By merging all our resources we can develop and maintain the cyber security we will need as technology races to become something new on a continuous basis. It is this joint unity that will continue to improve their strength wish us tonight.

Another thing we must do to strengthen our cyber posture is to enhance and inform decision-making using streamlined, inclusive and transparent governance across the enterprise. Effective governance is imperative in light of recent data breaches at all levels of government as well as the private sector. In addition to improved methods we must also do everything possible so that we may advance the science of cyber to transform our Energy Enterprise.

This will require not only commitment but also funding to continue to develop initiatives and methods to protect our data. As these resources continue to grow we must also advance our analytics, forensic and incident response capabilities. As we move forward we must also develop measurements for success in the implementation of our plans as well as ways to enhance decision making, ways to communicate value and also to ensure accountability.

Cyberattack is a real threat in today’s world. Therefore, protection of our data and our security is imperative. An attack is not as simple as someone making a physical attack against an enemy like it once was. Now an attack to a person, organization, or nation’s security is done with the touch of finger to a keypad or flick of the wrist, depending on the intrusion made on the victim.

There are new attacks almost as quickly developed as are new technologies. The DOE’s goal is to stay at the forefront of this threat so that it can be quickly defeated, even as new threats evolve. We have a history of success so I have every confidence that we will continue to succeed in this endeavor.

The data we work with crosses borders of departments, levels of government, it crosses subject matter and it crosses from government to private sector to international organizations. In order for our cybersecurity to be successful we must be able to cross all these lines to communicate and to share information in how to battle for this cybersecurity and to do so quickly and efficiently.

We are committed to winning this battle against our cyber security. We are one nation and will work by combining our resources so that we will overcome this cyberattack and safeguard our nation’s most important information. It is within our reach to overcome the danger of this mostly unseen attack. And, we are committed to seeing it’s destruction upon our cyber security.

Because of the nature of the work that we do, we are seasoned in working with other agencies and other departments for our cyber security. I know that we have the ability to overcome this challenge. I know that if we stand in unity, we will see the undoing of our largest known enemy. We will work together and we will overcome this modern day threat to our data and our security. We will continue working so that as technology changes we will keep up with it and maybe a little ahead of it so that we will not be caught unawares when an attack happens, for happen they will.

Wars are not just fought on the battlefield any longer. They are fought in the confines of a computer, where one group of people does everything in their power to steal or destroy the data of an opponent. The victims of one of these attacks may never see the damage done until it is too late to stop it. That’s why we must be proactive in our attack against a cyber threat. The information that we have has been entrusted to us by its owners and we must do all we can to protect it, just as surely as our early settlers were proactive in their protection of our nation from the variety of physical attacks they endured.

The important thing is that we must band together, agency with agency, government with private sector and departments with departments so that we can present a united front and cyber attackers will know that it is a waste of time to bother with attacking us, because we are prepared to do battle and have our safeguards in place so the enemy can’t harm us.

We have the goals set forth. We have the resources at our disposal or we know where to find them. But, most of all we have the human element of determination that we will succeed in this battle to protect the data of our nation, our organization, our friends, family and neighbors and we are home. Now we will do whatever is necessary to protect and defend the home we have fought so hard to build and develop.

That determination, at times a uniquely American attribute, has led our nation to victory many times in our history because we simply refused to give up. That is true in this case as well. We know the challenges to our cyber security and will not fail to protect it. We will do whatever is necessary to protect our cyber safety just as we have always do what is necessary to protect our physical safety.

I know we will succeed because I can see the looks of determination and tenacity on your faces. You know this victory is within our grasp. You know we can win this war of technology, and you will get up each day and put your best foot forward in order to gain victory in this battle. We will protect the data and information of our organization and those we partner with in this day of information processing.

You can be proud of the successes of your past, but it is now time to look to the future and see what great victories stand ahead of us. If you haven’t already, prepare yourself for battle and be ready to do whatever is required of each of us in this battle.

Thank you