General John Kelly, the SOUTHCOM commander, said: ''JSTARS is especially important, providing a detailed maritime surveillance capability that is unsurpassed.''

To give you a comparison, a single JSTARS sortie—a single plane—can cover the same search area as 10 maritime patrol aircraft sorties. But the future of this platform is in jeopardy. As threats against our Nation have evolved, JSTARS has too. But there are only 16 of these planes covering our needs worldwide over the last 25 years. We have relied on JSTARS for 25 years to protect our men and women whom we put in harm's way—to protect them while other people are trying to do them harm.

Unfortunately, in the last 25 years, these planes are beginning to wear out. They are reaching the end of their service life. These planes have been in service since the early 90s. But even then, these planes weren't new when the Air Force acquired them. Each plane on average had over 50,000 hours when we bought them. The average age of the fleet is 47 years.

If you look at just one example in the JSTARS fleet, there is one aircraft that had 16 different owners or lessors over that time before it became a JSTARS, including Pakistani International Airlines and Afghan Airlines. I think it is very ironic that today that very plane flies oversight missions over those two countries.

As these planes near the end of their service life, they are spending more and more time in depot maintenance. More maintains is more costly. Dramatically increased maintenance time is threatening aircraft availability and mission readiness. This in turn impacts the number of JSTARS that can be put into mission at any one time and be out in the combatant commands while doing their job, while day by day the demand from combatant commanders for JSTARS grows.

What is more concerning is that as JSTARS near the end of their service life, as you can see on this chart, there is a gap. If we do nothing, we will have a gap of 10 years. The best we could do starting today is to shorten that gap to 4 years. This is a gap we cannot allow to happen.

This chart shows the declining availability of the current fleet down to zero by 2023. It also shows that under the current plan—pending DOD approval and funding—the replacement fleet does not even come online until 2023, meaning we will have a 10-year gap. They don't get back to full strength until around 2027—again, the 10-year gap. Due to the increased maintenance requirements of this aging fleet, JSTARS is already at a point where we only have about half the fleet available to fly at any point in time. Even if we extend the service life of JSTARS and accelerate the replacement, we can only narrow the gap to 4 years. This is unacceptable.

I have talked about the planes. Let me talk about the men and women who man those planes, who service those planes, who keep those planes in the air. These are talented professionals. I have met with them. They are dedicated professionals, protecting our soldiers on the ground. They are committed to this mission, but they have to have our help. The men and women on the ground in Iraq, Afghanistan, and around the world deserve our help. But when it happens to have a gap like this, our irresponsibility as a Congress and as military leadership shows up.

We cannot allow this to happen. Recapitalization for the JSTARS fleet needs to happen, and it needs to happen right now. As these aircraft age, depot maintenance is not only more costly but also keeps these aircraft, which are in high demand for every combatant commander, from fulfilling their mission fully and putting our soldiers on the ground in mortal danger. This is precisely where we see the debt crisis and global security crisis intersect.

In the last 6 years, I have spoken about this before, but we borrowed 40 percent of what we have spent as a Federal Government. This puts our ability to support a strong foreign policy backed up by a strong military in jeopardy. As Admiral Mullen, former Chairman of the Joint Chiefs of Staff, once said, the greatest threat to our national security is our own national debt.

The JSTARS Program is an example of how our debt crisis is impacting our ability to fulfill our mission requirements. JSTARS recapitalization, which would replace these planes over time, is the No. 4 priority within the Air Force. The other three priorities ahead of it are very valid, but very expensive platforms.

Just last month, the Air Force acquisition chief, Assistant Secretary LaPlante, said that the JSTARS recap might get scrapped thanks to sequester and tight budget constraints. Again, this is a result of our fiscal intransigence and poor planning by military leaders. This prohibits us from meeting the very basic needs of our men and women on the ground who depend on this critical platform to protect them and provide overarching eyes and ears in the battle space. This should not have happened. The intransigence of Congress over the last decade and the intransigence of our military leadership and procurement planning are all at fault. We can fix this.

This week I am joining Senator ISAKSON and at least 11 other Senators in writing to Secretary of Defense Carter about the importance of funding for the next fleet of JSTARS in next year's budget request.

I wish to thank the defense appropriators as well as the Armed Services Committee for their support for this critical platform and mission. I look forward to continuing to work with them to support JSTARS. Not only do we need to ensure the new JSTARS fleet is funded, but this needs to be done fast. As I said, if we do nothing today, we have at best a 4-year gap, not to mention the problem with the planes. What do we do with these professional military men and women who are irreplaceable—pilots, navigators, engineers, technicians, mechanics, schedulers, and computer experts. This is a capability we cannot do without.

Not only do we need to ensure that the new JSTARS fleet is funded, but again this has to happen immediately if we are going to manage this gap. This gap in capability that we see on this chart will become a reality if the pace of recap doesn't change. We need a faster solution. This chart shows why this recap needs to be a rapid acquisition program and we need to get on that immediately.

We need to ensure that this critical platform stays in theater. Our combative commanders demand it, our troops on the ground depend on it, and they certainly deserve it. We cannot allow Washington's dysfunction to put our men and women in combat theaters in further danger. This needs to get fixed, and it needs to get fixed right now.

I yield my time.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Mr. CARPER. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

TRIBUTE TO FEDERAL EMPLOYEES

U.S. COMPUTER EMERGENCY READINESS TEAM

Mr. CARPER. Mr. President, I mentioned to the Presiding Officer in our brief conversation before I came to the podium that one of the things I try to do every month or so is come to the floor, usually when things are slower and there is not a lot going on, to talk about some of the folks who work for us and serve our country in the Department of Homeland Security.

Earlier this week, as my colleagues may recall, an outfit called the Partnership for Public Service released an annual report in which they rank the best places in which to work in the Federal Government. The report is based on surveys that are conducted literally by hundreds of thousands of Federal employees. This year it showed an increase in overall employee morale for the first time, I think, in 4 or 5 years. That is good news.

Despite the progress that appears to have been made in a number of Federal agencies, not all but many components of the Department of Homeland Security continue to struggle to make their employees feel good about their work and what they do for the rest of us.

I know the Secretary of the Department, Jeh Johnson, and his team have taken a number of significant steps to make the Department a better place to

work for current and future employees. They do outreach and get input from their employees as to what needs to be done to enable them to feel better about the work for greater job satisfaction, to make them want to come to work. I would also say today that the Congress—those of us who serve in the Senate and the House—also has a responsibility to help improve morale, not just at the Department of Homeland Security but in the Federal Government at large.

Considering the fact that we began 2015 with a fight in this body right here over whether we should even fund the Department, I don't believe those of us in the Senate or in the House are doing all we can do, that we are doing our part well. As I said earlier, that is why I come to the Senate floor on a number of occasions throughout the year to highlight some of the extraordinary work done every day by the dedicated men and women at the Department of Homeland Security.

Today I rise to recognize no one individual. Usually I pick one or two people who have done extraordinary things with their lives, but today I am going to focus on a whole team of people who do important work every day to defend our Nation from the growing and evolving threat our country faces in cyber space.

It seems as though we don't go a week without hearing about another major breach at a business or a government agency. We are under unrelenting attack from all over the world—in some cases from sovereign nations, in other cases from criminal organizations, and in other cases just from pranksters. Over these past few years, we have seen major attacks on the Office of Personnel Management, on a great many banks and other businesses, and even the email of the Director of the Central Intelligence Agency. These attacks make clear that the threats we face online are complex, and unfortunately we will be struggling with how to deal with them for the foreseeable future.

Fortunately, in Congress we have been making some progress combating these cyber threats through legislation. Last year we passed cyber security legislation—four bills in fact—out of the Committee on Homeland Security and Governmental Affairs. These four bills were aimed at strengthening the ability of the Department of Homeland Security to perform their cyber security mission.

Among those bills was one to update how our government protects its own networks. This bill includes language clarifying the role the Department plays in overseeing and enhancing security and other agencies. Two other bills gave the Department some of the tools it needs to strengthen its cyber security workforce, and just last month the Department of Homeland Security announced that it now seeks to hire up to 1,000 new cyber security employees over the next 6 months using the new authorities we have given them.

We also passed legislation that codified the cyber operations center at the Department. It is called the National Cybersecurity and Communications Integration Center, affectionately known as the NCCIC. Our legislation—which former Senator Dr. Tom Coburn and I coauthored, supported by many in our committee and outside of our committee—gave the NCCIC the strong legal foundation it needs, that it lacked, in order to do their job and engage with the private sector in a joint effort to better secure critical cyber networks.

I think we have made real progress on cyber security legislation this year as well. I think we are maybe poised to do even more. I would like to use a football analogy. The team flips a coin and somebody receives and somebody kicks the ball. Receiving takes the ball maybe deep in their own territory, and then they march down the field across the 50-yard line into the other team's territory, then they get to the 20-yard line, and then moving closer to the other team's goal line, they would say they are in the red zone. In terms of our march on cyber security legislation here and in the House, thanks to the good work of the Intel Committee here and the Committee on Homeland Security and Governmental Affairs as well, we are not just in the red zone, we are inside the 10-yard line and it is first down and goal to go.

Unfortunately, the clock is running out and we don't have forever to get the job done, but if we are smart and don't give up, we can have a real success for the American people in strengthening our cyber defenses in a real way.

The legislation we passed this fall was called the Cybersecurity Information Sharing Act, and it represents a collaboration on a number of cyber security issues. In the bill the Department of Homeland Security plays a central role as they interface between industry and the government. The bill also includes provisions to enhance the cyber security program at the Department of Homeland Security known as EINSTEIN, which uses classified threat intelligence to protect all of our civilian agencies.

I am mentioning all of this legislation to show the critical role or underline the critical role the Department of Homeland Security plays in security for our Nation. At the center of the Department's cyber security operation is the U.S. Computer Emergency Readiness Team, which is also known as US–CERT.

To my left is a picture of our President, and the handsome fellow he is speaking to is a fellow named Jeh Johnson, who is the Secretary of the Department of Homeland Security, a role he has filled for I believe most of 2 years now. I think he is doing a splendid job, with the great support of the Deputy Secretary there, Alejandro Mayorkas, and a couple of thousand people who are committed to defending our homeland.

This is a picture of the President addressing, along with Secretary Johnson, the employees at US–CERT. I think it was taken earlier this year. Again, US–CERT—the U.S. Computer Emergency Readiness Team—is the main operational team within the NCCIC. It is the operational team within the NCCIC itself.

What do they do? They pool information and they share that information throughout the Federal Government. The US–CERT also shares information with our partners in the private sector across the country and with our allies around the world. It is an important job. It is not a job that is done for 5 days a week, 8 hours a day. It is a 24-hour-a-day, 7-day-a-week operation, and these men and women work to stay ahead of the bad actors who are trying to steal our personal information and trying to really harm our economy. In some cases they are plotting to damage our critical infrastructure such as our electric grid, our financial systems, and our communications systems.

US–CERT was established 12 years ago as the Department of Homeland Security was first being stood up. The mission of US–CERT is simple, I think: to make the Internet a safer place for everyone by helping to improve cyber security across the country. I will say that again. The mission of US–CERT is very simple—not easy but simple. It is to make the Internet a safer place for everyone by helping to improve cyber security across our country. To do this, US–CERT operates a wide variety of programs. These programs include several information sharing collaboration programs, incident response teams that provide onsite assistance to attack victims, programs such as the EINSTEIN intrusion detection and prevention system to protect Federal agencies, education and awareness programs, and deeply technical forensic analysis. The US–CERT partners with a wide variety of organizations. Among them, they partner with powerplants and utilities, they partner with financial institutions, they partner with software companies, with researchers, and they partner with certain teams in other countries and other cyber operation centers such as those over at NSA, the National Security Agency, and the FBI as well.

When a major attack occurs in the Federal Government or the private sector, the men and women at US–CERT mobilize to travel to the victim's location. They help mitigate the attack. They help to strengthen the victim's cyber systems, and then they communicate with their partners so everyone can secure their systems against similar attacks. We learned from that bad experience, and hopefully we can help reduce the likelihood that someone else will suffer a similar fate.

Earlier this year, when the Office of Personnel Management discovered a

data breach of personal data belonging to millions of Federal employees, they called the NCCIC and asked for its team of experts. US–CERT was deployed to play a central role in, first of all, investigating the attack but also in responding to that attack. For the next 4 months, the team worked literally around the clock at OPM to assess and to monitor Federal networks and to develop new protections against this type of intrusion that OPM had experienced.

Now, once US–CERT realized that other Federal agencies were also vulnerable to this kind of a breach, they immediately shared the indicators of the attack with network analysts across the Federal Government. This allowed other Federal agencies to scan their systems and to make sure they had not been compromised by the same hacker and to be on alert for that hacker's attack.

Because of the scale and impact of the OPM breach, which I think actually ended up affecting more than 20 million people, the US–CERT team worked long hours to make sure they could provide guidance to Federal agencies as quickly as possible so they could protect their networks from similar attacks and prevent the attacker from using the information they obtained against us. Their work not only strengthened the Office of Personnel Management's cyber security posture, it also bolstered cyber security across the entire Federal Government.

US–CERT and all the cyber warriors at the NCCIC work tirelessly every day to out-think and out-innovate our cyber enemies. The legislation we enacted last year and the bill we are working hard to send to the President this year with great bipartisan support here in the Senate and the House as well puts the Department of Homeland Security in the spotlight and entrusts them with ever-greater responsibility for years to come. We in Congress recognize the critical role US–CERT plays in strengthening our Nation's cyber security, and we must continue to support these hard-working men and women in their mission.

Mr. President, I will close by telling a story. I have told this story before, but it is a good one, and it is certainly germane to what we talked about here today.

A couple of years ago, I was listening to a radio station on my way to the train station in Delaware, and I caught NPR news right at 7 a.m. as I made my way to the train station in Wilmington. On the news that morning, they gave a report about an international survey that was taken where they asked thousands of people in different countries and here: What is it about your work that you like? What is it about your work that makes you like your job or not like your job?

Some of the people who were asked said: Well, the thing I like about my job is I like getting paid—not that they are in it for the money, but they like getting paid. Others said they like vacations. Some people said they had health care. Others said they like the folks they work with. Other people said they like the environment—a beautiful place like this in which they work. But what most people said they liked were really two things: No. 1, they knew the work they were doing was important, and No. 2, they felt as though they were making progress. Think about that. They knew the work they were doing was important and they felt as though they were making progress.

Well, there is probably nobody in our country—at least working within the Federal Government—who does work more important than the folks at the Department of Homeland Security. The House and the Senate have worked in recent years to strengthen the ability of the Department of Homeland Security, including the US–CERT team, to be able to do their job even better.

My hope is that in years to come, as we hear these annual reports on best places to work within the Federal Government, that we are going to find that the people at the Department of Homeland Security, including NCCIC and US–CERT, will be saying more and more: I like working here because I know the work I do is important, and I feel as though we are making progress.

This Senator would just say to everyone at US–CERT, thank you for all the good you do for us. Thank you for your service to this country. And to each of you, we wish you happy holidays and Merry Christmas. We would also say, here is hoping that we will all have a more peaceful new year. I think the American people are ready for that. I know the Presiding Officer is, and so am I.

With that, I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER (Mrs. FISCHER). The clerk will call the roll.

The senior assistant legislative clerk proceeded to call the roll.

Mr. SANDERS. Madam President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER (Mrs. ERNST). Without objection, it is so ordered.

(The remarks of Mr. SANDERS pertaining to the introduction of S. 2391, S. 2398, and S. 2399 are printed in today's RECORD under ''Statements on Introduced Bills and Joint Resolutions.'')

Mr. SANDERS. I yield the floor.

The PRESIDING OFFICER. The Senator from Connecticut.

THIRD ANNIVERSARY OF SANDY HOOK TRAGEDY

Mr. MURPHY. Madam President, next week we will mark the 3-year anniversary, for lack of a better word, of the massacre at Sandy Hook, CT. Senator BLUMENTHAL will be joining me on the floor momentarily. I wanted to come to the floor to speak to our colleagues for a few moments about what this week will mean to us in Connecticut and the challenge it presents to all of us.

I want to open by speaking about one of the young men who perished that day—a little first grader by the name of Daniel Barden. Daniel was a really, really special kid. I talk about him a lot when I am speaking on Sandy Hook because I have gotten to know his parents pretty well over the years, so I feel like I know Daniel pretty well. Now that I have a little 7-year-old first grader at home, too, I, frankly, feel closer than ever before to the families such as the Bardens who are still grieving.

Daniel had this sense of uncanny empathy that, now as a father of a 7-year-old, I know is, frankly, not normally visited upon children that age. Daniel just loved helping people in big and small ways; he was so preternaturally outward in his sympathy for others.

There is a story his dad likes to tell about the challenge of going to the supermarket with Daniel because when they would leave, Daniel always liked to hold the door open for his family. But then he wouldn't stop holding the door open because he wanted to hold it open for all of the rest of the people who were leaving the grocery store. So the family would get all the way to the car, and they would look back and they wouldn't have Daniel because he was still holding the door open. It was small things like that that made him such a special kid.

His father, Mark, wrote one day: ''I'm always one minute farther away from my life with Daniel, and that gulf keeps getting bigger.'' His mother, Jackie, in the months and years following Daniel's death, developed a habit of what grief counselors call defensive mechanisms. She would sometimes pretend that Daniel was at a friend's house for a couple hours, simply in order to give herself the strength to do simple household chores like cooking dinner or returning emails. The only way she could do it is if she pretended for a small slice of time that Daniel was actually still alive.

It is hard to describe for my colleagues here today the grief that still, frankly, drowns Sandy Hook parents and the community at large. It is total, it is permanent, and it is all-consuming. But for many of those parents and many of those community members, the grief now is mixed with a combination of anger and utter bewilderment, all of it directed at us, in the Senate and in the House of Representatives.

On December 14, Adam Lanza walked into Sandy Hook Elementary School armed with a weapon that was designed for the military—designed to kill as many people as quickly as possible. He had 30-round magazines, not designed for hunting or for sport shooting but to destroy as much life as quickly as possible. Importantly, he left at home his lower round magazines. And the design of his weapons worked—to a tee. In approximately 4 minutes, he discharged