Talk Nerdy To Me

August 2021

Tokyo's Olympic Medals Are Made Entirely From Recycled Gadgets

This year, the Tokyo Organizing Committee of the Olympic and Paralympic Games was in charge of presenting the gold, silver, and bronze medals—and they're all made from recycled electronics. The Committee says it decided to create sustainable medals in an effort to build "an innovative future for all."

Tokyo 2020 Medal Project officials shared that they hoped the results of the upcycling would create a lasting legacy and "contribute to an environmentally friendly and sustainable society."

The process has been in the works since early 2017, when Japan announced it would collect old electronics and repurpose them into medals. Since then, the organizing committee has gathered over 47,000 tons of tech waste and more than five million cell phones in an effort to make the Games more sustainable.

The committee collected around 70 pounds of gold, 7,700 pounds of silver, and 4,850 pounds of bronze—all from various donated electronic gadgets—to fashion approximately 5,000 medals for this year's Games. The Japanese government recycled any source materials that weren't used to make the medals.

Tokyo took inspiration from the 2010 Vancouver Winter Olympics, which implemented a similar method of reusing electronics (like TVs, computers, and keyboards) for their medals. For that effort, the Vancouver-based metal company Teck Resources teamed up with the Canadian Mint to create approximately 1,000 medals.

Source: https://www.popularmechanics.com/

Federal Cybersecurity Defenses Not Strong Enough to Protect American Data

Federal agencies responsible for safeguarding the security and personal data of millions of Americans have failed to implement basic defenses against cyberattacks, according to a report from Senate investigators released Tuesday. The agencies earned a C- report card for falling short of federally-mandated standards in the 47-page report by the Senate Homeland Security Committee. The report also concluded that Americans' personal information remains at risk in the wake of a slew of high-profile cyber attacks and evaluated two years of inspector general reports.

The audit accuses eight critical agencies, including the Department of Homeland Security (DHS), the State Department and the Social Security Administration (SSA) of relying on outdated systems, ignoring mandatory security patches and failing to protect sensitive data such as names, date of birth, income, social security numbers and credit card numbers.

In 2020, the White House reported 30,819 information security incidents across the federal government— an 8% increase from 2019 – according to the report, which also evaluated the Department of Transportation (DOT), the Department of Housing and Urban Development (HUD), the Department of Agriculture (USDA), the Department of Health and Human Services (HHS) and the Department of Education. According to the report, HUD's top watchdog found an "unauthorized 'shadow IT'" system on the agency's network that "existed without approved authorities to operate."

In a test of its cyber defenses, the State Department could not provide documents accounting for 60% of employees who had access to the agency's classified network. The report found the agency "left thousands of accounts active after an employee left the agency for extended periods of time on both its classified and unclassified networks." The top watchdog at the Department of Education retrieved "hundreds of sensitive personally identifiable information files, including 200 credit card numbers without the agency detecting or blocking it."

At the Department of Transportation, the Inspector General had no record of nearly 15,000 IT assets owned by the department including, "7,231 mobile devices, 4,824 servers, and 2,880 workstations."

"All agencies failed to comply with statutory requirements to certify to Congress they have implemented certain key cybersecurity requirements including encryption of sensitive data, least privilege, and multi-factor authentication," said the report.

Tuesday's review outlines failures to comply with the Federal Information Security Modernization Act (FISMA) of 2014 and comes on the heels of two major security incidents breaching multiple federal agencies. In April 2021, Chinese state-sponsored hackers breached five federal agencies through vulnerabilities in products from a popular, Utah-based software company, Pulse Connect Secure. Russian-linked criminals compromised nine federal agencies and 100 private sector groups through a supply-chain hack of Solarwinds, first discovered in December 2020.

"From SolarWinds to recent ransomware attacks against critical infrastructure, it's clear that cyberattacks are going to keep coming and it is unacceptable that our own federal agencies are not doing everything possible to safeguard America's data," Senator Rob Portman from Ohio said in a statement.

"This report shows a sustained failure to address cybersecurity vulnerabilities at our federal agencies, a failure that leaves national security and sensitive personal information open to theft and damage by increasingly sophisticated hackers," added Portman, the ranking member of the Senate Homeland Security Committee. "I am concerned that many of these vulnerabilities have been outstanding for the better part of a decade."

The bipartisan report compiled by congressional investigators draws information from Inspector General reports issued by federal agencies' top watchdogs in fiscal year 2020. It follows the subcommittee's initial report in 2019 that evaluated the same eight agencies.

Since the 2019 audit, investigators found only the Department of Homeland Security (DHS) established an effective information security program. "Three agencies— the Department of Transportation (DOT), Department of Education, and Social Security Administration (SSA)— showed very little improvement since the Subcommittee's report in 2019," the report added.

Tuesday's evaluation also found that EINSTEIN, DHS's flagship cybersecurity program for federal agencies, suffers from "significant limitations in detecting and preventing intrusions." Congressional investigators recommended an "update" to Einstein that justifies its cost. Authorization of the program with a price tag in the billions is set to expire in 2022.

The report also makes several suggestions aimed at boosting coordination, including a recommendation that the administration assign a primary office to develop and implement a cybersecurity strategy for the federal government.

Continued on Page 4

Our CEO Is A Published Author

Stay one step ahead of cyber criminals to protect your business, your customers, and your money!

In Jason's first published book, he talks about why cybercrime today cannot be ignored and why your network and data are cyber criminals' #1 target!

Learn all the ways to protect yourself and your data. Contact us today for your copy of *Inside The Hacker Mind.*

Happy Birthday Amy and Carter!!

Thank you for everything you do! Enjoy your birthday month!

Federal Cybersecurity Defenses - Continued

“There isn’t currently a single point of accountability, government-wide, for cybersecurity,” a committee aide said. “Each agency is responsible for its own cybersecurity, but government-wide it’s not clear who is responsible for coordinating the whole strategy.” Lawmakers have not collectively decided on who should quarterback the nation’s cybersecurity, but cybersecurity experts have pointed to DHS’ cyber arm launched in 2019. The Cybersecurity and Infrastructure Security Agency (CISA) is currently charged with disseminating actionable information to both the federal agencies and the private industry to attempt to prevent repeat cyber-attacks.

“Government-wide cybersecurity is highly federated,” a committee aide said. “That federalization, that balkanization of cybersecurity across federal agencies has been a persistent problem. It’s probably a large part of why we’ve seen such performance issues at each of these agencies.” Last month, the White House swore in its inaugural National Cyber Director. The expanded role building on the White House cybersecurity coordinator position eliminated under the Trump administration, was created as part of the most recent National Defense Authorization Act.

In his first public appearance, Director Chris Inglis said he plans to ensure digital infrastructure used by the 102 civilian components of the federal government have the “right technology [and] the right practices” to achieve “unity of effort and unity of purpose,” at a virtual panel convened by the Atlantic Council, Monday.

Investigators also recommended that Congress update the Federal Information Security Modernization Act of 2014 “to reflect current cybersecurity best practices” and require federal agencies and contractors notify CISA of certain cyber incidents. Senator Peters and Portman are working on legislation to update the now outdated cybersecurity standards, committee aides confirmed to reporters. “I think we’re hopeful that we can get that done and introduced this Congress,” an aide added.

Source: https://www.cbsnews.com/

FUN FACT!

Gmail blocks an average number of 100 million spam email messages daily.