FRCSW information technology specialist Tamika Clay-Jefferson is presented the 2018 A. Bryan Lasswell Award for fleet support by Rear Adm. Dan Dwyer, commander, Carrier Strike Group Nine, October 23 at the Town and Country Hotel. The award recognizes individuals who have provided exceptional support through in-service engineering procedures or technical innovation to the armed services based in San Diego. (U.S. Navy photo)

NAVAL AIR STATION NORTH ISLAND, Calif. - Tamika Clay-Jefferson, an information technology specialist for Fleet Readiness Center Southwest (FRCSW), is the recipient of the 2018 A. Bryan Lasswell Award for Fleet Support.

Sponsored by the National Defense Industrial Association and named for Marine Corps Maj. A. Bryan Lasswell, the award recognizes individuals who provide exceptional support to the Navy, Marine Corps or Coast Guard forces based in San Diego.

In 1942, Lasswell, who was a translator and cryptologist, deciphered communications of the Japanese Navy, which proved vital to the American victory at the Battle of Midway Island.

In 2015, Clay-Jefferson joined the FRCSW Information Technology and Management Department and works as the command’s information systems security manager (ISSM).

A year earlier she wrapped up a 14-year naval career where she initially served (not unlike
Lasswell) as a cryptologic intelligence technician, until the rate merged with information systems technician in 2006.

Earning a bachelor’s degree in information technology management along the way, Clay-Jefferson found herself challenged to apply her experience and education to improve FRCSW’s cybersecurity program.

“When I started working here I wasn’t in the position that I am in now. I was watching and learning to see how we did business. I noticed that we were deficient in a number of areas, and I’m now in a position to affect change,” she said.

FRCSW’s cybersecurity guidelines are governed by a myriad of authorities including the National Institute of Standards and Technology’s (NIS) Risk Management Framework (RMF), the Department of Defense and the Department of the Navy.

“We have to be in line not only with the DOD and DON standards, but also follow whatever the SECNAV puts out,” Clay-Jefferson noted.

“All of these things have a position in the cybersecurity workforce. So our job is to make sure we understand all of those requirements, and that we create command policy, instructions and guidelines to make sure that we’re in line.”

In addition to creating a mandated cyber-awareness brief for new employees and improving computer security awareness, Clay-Jefferson targeted command systems in need of current Authority to Operate (ATO) status.

“We have so much gear that doesn’t have ATO, that right now we are in the discovery phase of identifying all of our equipment and systems that will need ATO. If they need updated, we’ll provide that to ensure that we are keeping up with Navy policy,” she said.

Systems that are tested and verified to meet the requirements of their Information Assurance (IA) programs are forwarded to the DOD’s automated Enterprise Mission Assurance Support Service where they are assessed and granted ATO validation.

FRCSW’s research, test, development and evaluation (RTD&E) labs are examples of areas with systems in need of ATO authorization to operate.

“We have adapted the Risk Management Framework (RMF) process that has a list of all their equipment and structure and it’s basically giving the ability to ‘go live’ and do the job because all of the DOD, DON and NIS standards are met,” Clay-Jefferson said.

“By definition the cyber office is supposed to have oversight of all the command’s systems and that wasn’t really happening; so we established relationships to let them know that we are here to support them and whatever they need.”
FRCSW Employee Receives 2018 Lasswell Award for Fleet Support

As part of her ISSM duties, Clay-Jefferson works with the FRCSW Security Department to establish physical security procedures in the labs such as access control and gear to mask computer servers which should not be visually exposed.

Command-wide, security procedures developed last year targeting the use of government computers resulted in a 95 percent reduction in violations since March 2017.

“These decreased incidents refer to unauthorized plug-ins of personal cell phones and flash drives in government equipment, which also resulted in a reduction of viruses,” she said.

In the meantime, Clay-Jefferson and the cybersecurity team are preparing for a cyber-readiness inspection scheduled for February 2019. The week-long inspection is conducted by the U.S. Fleet Cyber Command by direction of the Defense Information Systems Agency.

The inspection will target technical and traditional security issues and the security culture of the command.