

Computer Incident Response Team



Policing the U.S. Postal Service's computer network, the third largest in the United States, is no small job; however, that is the mission of the USPS Computer Incident Response Team (USPS CIRT). This team of incident response professionals triage potentially dangerous issues on the USPS computer infrastructure that could adversely affect the Postal Service's mission. Based in Raleigh, North Carolina and staffed by five postal employees and one USPS OIG Computer Crimes Unit (CCU) special agent, the team interacts daily with the postal Information Technology Headquarters and field offices to fully identify and mitigate security issues. The USPS OIG special agent works with the USPS CIRT team to review incoming information security issues. This cooperative effort has resulted in the initiation of dozens of allegations for OIG field agents. During fiscal year 2007, the USPS CIRT reviewed more than 1,200 information, security-related issues and fielded more than 1,600 calls. In addition, CCU's close association with USPS CIRT has increased the OIG's ability to obtain postal data in support of various investigations. This has drastically reduced the time it takes to retrieve postal data. What used to take weeks now takes days!

During the spring of 2007, the Postal Service computer network suffered a mysterious security policy modification, which affected thousands of computers, rendering them unusable. This critical computer incident resulted in damage to

thousands of postal computers and hundreds of thousands of dollars in losses to the Postal Service. CCU and USPS CIRT immediately responded to mitigate the situation. They provided emergency measures to retain computer services within the enterprise and prevent the spread of the modified policy settings. Logical suspects were identified and painstakingly eliminated. Eventually the culpable party confessed. This close cooperation and the coordinated efforts of CCU and USPS CIRT resulted in the successful conclusion of this serious incident.