# Summary: Investigation of NPS-GCNP SCADA SYSTEM

**Report Date: August 7, 2014**

OIG investigated allegations that the Supervisory Control and Data Acquisition (SCADA) system at Grand Canyon National Park (Park) may be obsolete and prone to failure. In addition, it was alleged only one Park employee controlled the system, increasing the potential for the system to fail or become unusable.

The SCADA system is a private utilities network that monitors and controls critical infrastructure elements at the Park. Failure of the system could pose a health and safety risk to millions of Park visitors. Due to potential risks that system failure posed, we consulted with the U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and asked that they assess the overall architecture and cybersecurity of the Park's SCADA system.

ICS-CERT conducted an onsite review and issued a report outlining the weaknesses it found at the Park's SCADA system, including obsolete hardware and software, inadequate system documentation and policies, insufficient logging and data retention. We provided a copy of ICS-CERT's assessment report to the National Park Service for review and action.

*This is a summary of an investigative report that was issued internally to the U.S. Department of the Interior. This summary was posted to the web on December 2, 2015.*