

3439 Separate IT Network needed for Laboratory instrumentation

In light of the upcoming IT security changes, I have concerns about how our laboratory instrumentation will be integrated in this. Scientists do need instruments connected to the internet to update vendor software, receive alerts that something has gone wrong with an experiment or assistance with troubleshooting from a vendor. Our problem is there are software conflicts while running virus scans in the background, implementing updates and restarting computers during an experiment.

I would like to strongly encourage IT to consider having a totally separate network and email system for laboratory instrumentation (so alerts can be sent when needed) that can handle and address these needs. Our lab IT requirements are vastly different from typical office/desk work.

This is a critical issue. The ARS's mission is to do scientific research. If we cannot use the full capabilities of our instrumentation, of which ARS invested a lot of money into, it could limit our research abilities.

Agency Response

Thanks for your question, which raises two major points: a separate scientific network and the effect of cybersecurity rules on scientific computing. There's a lot of good news to report about a separate scientific network. We are putting in place a new, separate network that is to be used strictly for scientific data and applications. This is being done as a part of the ARS Big Data Initiative. You can find a summary of the ARS Big Data Initiative on our Intranet, Axon, at <https://axon.ars.usda.gov/Science%20Links/Pages/Big-Data.aspx>. You may recall that ARS contracted with a private firm, Bioteam, to conduct an assessment of scientific computing at ARS and to provide recommendations for future state-of-the-art scientific computing at ARS. Their recommendations were released in March of 2014 and are part of the materials that are linked to on the Axon Big Data page. They recommended that ARS should develop a separate scientific network to be used for scientific data transfers, a shared high-performance computing capacity to be available for all ARS scientists, and a Virtual Research Support Core staffed with experts in various computational specialties to enable ARS scientists to use the infrastructure. ARS Administrator Dr. Chavonda Jacobs-Young endorsed the recommendations in April 2014. Agency funding of \$5 million per year for the first five years of the initiative has been allocated to build and support the new infrastructure.

Over the last 18 months, a team led by ARS Associate Administrator Steve Shafer, Acting Chief Scientific Information Officer Doreen Ware, CIO Paul Gibson, and CTO Tom Houston have been coordinating implementation of this initiative. In addition, several working groups that involve numerous scientists and IT Specialists from across ARS program areas have been playing a key role to ensure that the environment is configured in a way that meets the diverse computing requirements of ARS scientists. ARS has also contracted further with Bioteam and Internet2 to establish the new network, called SCInet, and install and configure the high performance computing. As of the end of September 2015, the network is being tested in five of the initial six intended locations: Beltsville, MD; Ft. Collins, CO; Ames, IA; Stoneville, MS; and Clay Center, NE. The sixth location, Albany, CA, should be ready for testing in the next month. When operational, the network will be a completely separate network from ARSnet, connected instead to Internet2, which enables the high-speed data transfers (10 gigabits to 100 gigabits per second) necessary to move large amounts of data among ARS locations or with

collaborators, such as university-based colleagues, who are also connected to Internet2. At the heart of this new network is the high-performance computing cluster, located in Ames Iowa, at a lab operated both by ARS and APHIS. This resource, which is now in its initial testing phase with a group of scientists, will serve as a shared computing resource for ARS scientists to use for advanced computing needs. OCIO and Bioteam will also release a tool so those who are not at the six locations listed above will be able to use the network. Discussions about future developments will also need to consider which locations would benefit from expansion of the network. Further expansion can also include configuring access to SCInet from University-based ARS locations where Internet2 is already available.

It's important to recognize that ARSnet will still be used by many ARS scientists to support their work. It will still be our link to the Internet. Whereas Internet2 provides connections among research and other institutions that have joined the consortium, it's not the Internet and as such will supplement, rather than supplant, the Internet. The Internet that we know and use on a daily basis will still play an important role in supporting routine scientific and administrative activities. The need to manage cybersecurity issues will always be with us and along with it the challenge of ensuring that ARS science is not impeded by cybersecurity requirements. We are all aware of the reality that numerous cybersecurity threats exist and can too easily turn into cybersecurity incidents that lead to lost data, productivity, or cause other damage. As such, we'll always need to maintain an appropriate level of cybersecurity defenses for our network and computer-based resources. You make excellent points about the challenges to scientific computing that compliance with cybersecurity requirements can introduce. Appropriate cybersecurity and scientific computing are not incompatible, but they do require more coordination and planning than in other cases. As CIO Paul Gibson says, we need to "get the basics right" of cybersecurity, such as applying software patches, running software and network scans, and using more recent versions of software. Ensuring that we are "getting the basics right" also includes appropriate risk management, not simply applying limitations on our ability to use computers or networks. OCIO is ready to work with you or your IT specialists to help ensure that getting the basics of cybersecurity in place do not stand in the way of ARS science. OCIO can provide guidance to you or your IT specialists as to how to manage the timing of software patches, virus scans, etc. so as not to interfere with ongoing experiments. There are additional approaches that can be used, such as network segmentation, that can similarly help ensure that you can conduct the scientific computing you need while meeting appropriate security requirements. The two are not mutually exclusive but can be met with some planning and coordination.