**NSDD Policy on Remote Access to Operational Systems**

Jeffrey M. Knight, Adrian Pidlusky, Sabrina Ragaller, Paul Dimmerling

Office of Defense Nuclear Nonproliferation

National Nuclear Security Administration

U.S. Department of Energy

The Office of Nuclear Smuggling Detection and Deterrence (NSDD) rescinded *SLD Program Notice #27, Virtual Private Network (VPN) Policy* of August 2, 2010on April 8, 2020. That notice outlined a process to utilize VPN technology for remote access by NSDD stakeholders (DICCE Contractors, Subcontractor Communication Vendors, Laboratory Personnel and Subcontractors).

This policy provides new guidance. The risks of unmanaged and unauthorized access to operational Radiation Detection Systems (RDS) outweigh the benefits. Operational RDSs are defined as those operated by a partner. Such risks bring undue cyber, operational, and reputational risk to NSDD. In addition, remote access by NSDD stakeholders to assist partners with collection of daily files and system logs, preventive and corrective system administration, system patches and anti-virus definition files, diagnostics, and troubleshooting can slow transition of such capability and responsibility to the partner.

Please note, remote access by NSDD stakeholders is not required for meeting sustainability objectives and needs for support of RDS sites, and should not be used as, or considered a replacement of, local system administration by partner countries. NSDD management accepts responsibility for any resulting delay in resolving partner country requests for support.

Furthermore, NSDD recognizes that various forms of remote connectivity currently exist within certain NSDD RDSs (e.g., National Communications System, Daily File Upload Tool, partner established connections), whether installed by NSDD or not. This policy specifically addresses non-NCS and DFUT external ingress by NSDD stakeholders to RDSs. NSDD will continue to assess security of existing external RDS connectivity and promote partner cyber security capacity.

Hence, VPN usage is not permitted without explicit approval by NSDD management. NSDD strongly recommends alternative means of assisting in remote administration and technical troubleshooting. A simplified list of remote access alternatives is noted here:

* File transfer - portable media
  + Portable media (e.g., thumb drives) can transfer files to and from the RDS system.
  + File transfer should occur via dedicated media only. Dedicated media must be scanned for viruses. Personal media are forbidden within the RDS infrastructure.
  + An intermediate system with external/internet connectivity can transfer files from portable media.
* Audio and visual communication for consultation with local operational and technical staff
  + Remote advice and guidance may occur via telephone to provide constant communication with local staff.
  + Video links on non-RDS connected systems and devices (laptops, tablets) provide visual communication that can enhance voice support as well.
  + Virtual studio technologies used for remote NSDD training, workshop, and exercises, are available for facilitating consultations.
* In-person visitation
  + As travel conditions allow, contractor technical staff of local maintenance and other service providers may assist directly.

These forms of technical help require patience and preparation.

# Exceptions

NSDD management expects that alternative means of remote administration and technical troubleshooting will suffice for most cases.

NSDD stakeholders may encounter unusual or extreme circumstances and can consult with NSDD management on temporary, remote access considerations on a case-by-case basis.

Following approval of an exception, it is important to note that existing VPN technology may require upgrades, reconfiguration, or other administrative measures before enabling temporary remote access. It may take time to gain access, and careful planning will enhance the remote access request and solution.