



DHS CISA CSET Tool - Ransomware Option

Fellow InfraGard Louisiana Members,

The Cybersecurity and Infrastructure Security Agency (CISA) continues to make strengthening our nation's resilience from cyberattacks – against both the private and public sectors – a top priority. As part of this ongoing focus on ransomware, CISA is releasing a new resource focused on this ever-evolving threat. CISA released its [Ransomware Readiness Assessment](#) (RRA), the latest assessment module in its suite of Cyber Security Evaluation Tool (CSET®) products designed for Critical Infrastructure Industrial Control Systems (ICS) stakeholders.

As many of you know, CSET provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture. It is a desktop software tool that guides asset owners and operators through a step-by-step process to evaluate ICS and information technology (IT) network security practices. Users can evaluate their own cybersecurity stance using many recognized government and industry standards and recommendations.

The ransomware self-assessment is a unique stand-alone resource that can be downloaded from CISA's CSET GitHub page: <https://github.com/cisagov/cset/releases>. Included on the GitHub site, stakeholders will find training materials intended to assist those delivering the assessments in understanding how to present and document the new ransomware-focused engagement.

Thanks Phil Constantine For Sharing!!

**Best Regards / God Bless,
Lester Millet III, President InfraGard Louisiana**



Lester J. Millet III, LEM
Safety Agency Risk Manager / FSO Workgroup Chairman
Port of South Louisiana
171 Belle Terre Blvd.
P.O. Box 909
LaPlace, Louisiana 70069-0909
Office: 985-536-8300
Fax: 985-479-1643
Toll Free: 1-866-536-8300
Cell: 985-210-7518
Email: lmillet@portsl.com
web: www.portsl.com
"Proud Member of InfraGard"

(U) **Warning:** This document may contain information that is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO), and thus exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information, and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized private sector security officials without further approval from DHS.

Pursuant to the Electronic Communications Privacy Act (18 USC 2510-2521), the information contained within this email (including any attached files) is considered confidential, and intended solely for the named recipient(s). If you are not the named recipient, you may not read, distribute, copy, or alter this email. Views or opinions expressed in this email are those of the sender, and do not represent those of the Port of South Louisiana. If you received this email in error, please contact the sender (985) 536-8300, and delete the message. This email does not constitute an offer, acceptance, or contract amendment, unless explicitly stated as such, by the Port of South Louisiana. Warning: Despite precautions taken to ensure viruses are not present in this email, the Port of South Louisiana does not accept responsibility for any loss or damage arising from the use of this email and/or attachments