Regional Secure Information Sharing Pilot Project
At A Glance

The private sector members of the Multi-State Fleet Response Working Group are working with state/local government agencies on the East Coast to expedite the flow of sensitive operational information across multiple states during disasters in order to restore power and supply chain disruptions. The regional Secure Information Sharing Pilot is leveraging a proven, stable process to test secure operational information sharing within the electric, food and fuel sectors. This document provides a brief overview of the pilot.

Why Is This Pilot Happening?
Sharing information between private and public sectors is important when resolving operational issues within a multi-state region. Sharing sensitive operational information is still risky and requires a “trust framework” that is proven to reliable and secure; can allow specific, pre-approved state/local government individuals’ access; can be operated by the private sector; and will be trusted by the private sector if they are going to use it and sustain it through government elections, budget shifts, and retirements.

Who Are The Sponsors Behind the Pilot?
The All Hazards Consortium (AHC), the Transglobal Secure Collaboration Program (TSCP), DHS Science & Technology’s Cyber Security Directorate, the PIV-I / FRAC Technology Transfer Working Group, the Multi-State Fleet Response Working Group, and state/local government advisers on the East Coast Corridor Coalition (EC3) Working Group.

What is the Pilot Going To Do?
The Pilot will test the secure sharing of sensitive private sector operational information with specific state/local government operations professionals in law enforcement, emergency management, homeland security and transportation to support expedited power and supply chain restoration efforts and information sharing in the electric, fuel and food sectors.

What Is The Process?
40 Cyber ID cards using the PIV-I standard will be provided by TSCP to be issued to participants to test access to a digitally encrypted portal to share sensitive private sector operational information/files with government, and visa-versa. The process to be followed leverages a federally approved Personal Identity Verification process already being used by over 50 million stakeholders across the world in the aerospace industry via TSCP members.

Where Is The Pilot Being Conducted?
The Pilot project will involve private sector representatives from around the US along with state/local advisers from NC, VA, MD, WV, PA, NJ, NY, Baltimore/MD, Philadelphia/PA, Newark/NJ, Washington/DC and New York City/NY.

When Is The Pilot?
The Pilot project planning has been underway since early 2014 with Cyber ID cards being issued 1st QTR 2015. Pilot to run for 6 months (subject to change).

How Will People Participate?
The Pilot will engage two levels of participation: 1) Access to “sensitive information” will require a Cyber ID card; 2) Access to “non-sensitive” information (but still restricted to pilot project only usage) will require a username/password.
Pilot Program of the Multi-State Fleet Response Working Group

Online Resources:

1) Secure Information Sharing Pilot Video
2) Pilot Project Webpage w/ PIV-I Educational Information
3) DHS S&T PIV-I / FRAC TTWG Working Group
4) Cyber Solution – Secured Information Sharing Using “Verified Identity”