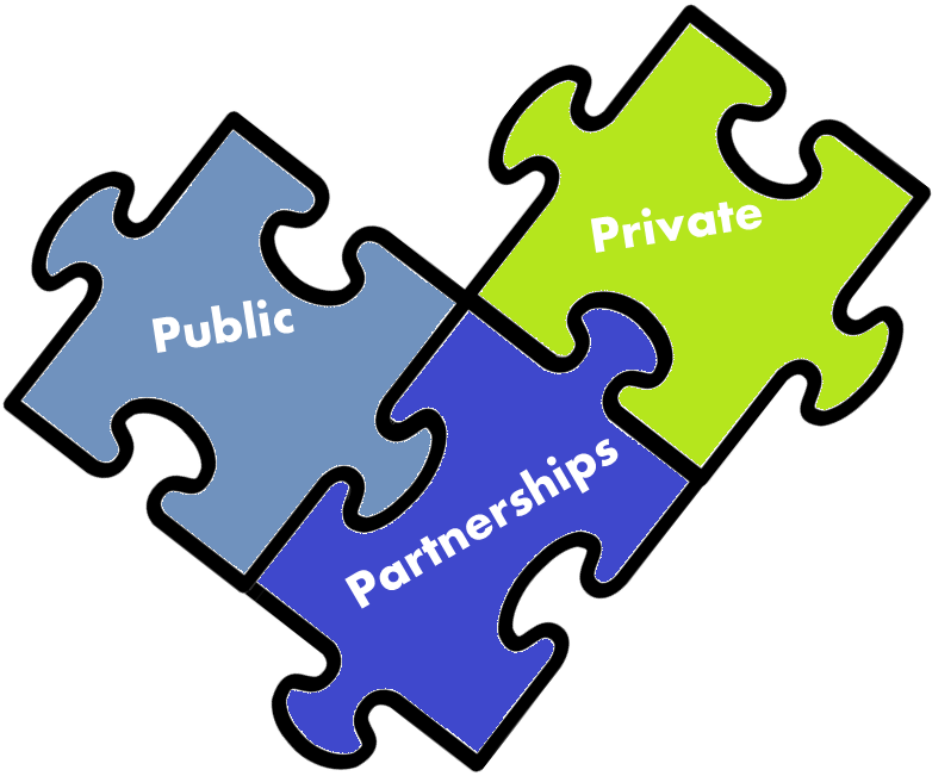
CASE STUDY #4:

Why Should Businesses Participate in Public-Private Partnerships for Cybersecurity?



DeBora King
CSIA 360 7980
Cybersecurity in Government Organizations (2172)
May 1, 2017

University of Maryland University College – Spring Semester, 2017

INTRODUCTION

Public-Private Partnerships have many definitions in common, but it is generally defined as contractually offering public assets and public services whose infrastructure is managed by a private partner. This type of infrastructure is also known as PPPs (APMG, n.d.). There is a need for more mandates surrounding PPPs. According to the Public Private Partnership Law Review, "there is no national legislative standard providing for public private partnerships," although enabling legislation with PPP involvement is required. In 2015, the Obama administration introduced a new initiative in renewable energy financing implementation of ARRA energy. The development and deployment was fully supported by the administration, but it is uncertain how future administrations will move forward. Initiatives pushed by the administration included loan programs for the Department of Agriculture biofuels project and the Department of Defense's renewable energy.

TYPES OF ACTIVITIES AFFILIATED WITH PPPs

Organizations that are leaders in the cyber defense initiative is the Federal Energy Regulatory Commission (FERC) which is an independent agency that's involved in the regulation of interstate transmission of electricity, natural gas and oil. In 2007. This agency gave NERC the authority to legally enforce reliability standards across the board (House, 2014). NERC developed the critical infrastructure protection program (CIP) to enforce compliance among owners and operators of bulk power systems. NERC-CIP standards are considered an exceptional foundation for cybersecurity defense. In addition to making cybersecurity a priority the framework suggests the following:

- Know
- Prevent
- Detect
- Contain and respond; and

- Recover

BEST PRACTICES

Best practices offered by Connecticut's cybersecurity utility guide are a great tool to follow. Below are some of their recommendations:

- Direct attention to and focus on these challenges – risk management and cyber secuity.
- Have an adequate cybersecurity budget to include procurement of hardware, software and skilled staff.
- Provide continued training for staff that follow the trends of the evolution of threats in technology.
- Continual auditing, testing, mock drills while utilizing outside assistance to strengthen deterrence.
- Utilize outside experts and sources to ensure full coverage where internal expertise is lacking.
- Sharing best practice by being an active participate in trade associate activities.
- Use National Institute of Standards and Technology framework (three parts).
    - The core
    - The profile
    - The Tiers

References:

APMG International (n.d.). Defining PPPs for the purpose of this PPP guide. PPP-certification.com. Retrieved from https://ppp-certification.com/ppp-certification-guide/11-defining-ppps-purpose-ppp-certification-guide

Werneck, B. and Saadi, M. (2015, March). The public-private partnership law review. Retrieved from http://www.kilpatricktownsend.com/~/media/Files/articles/2015/PPPEdwardsRiedyHafer2015.ashx

House, A. (2014, April 14). Cybersecurity and Connecticut's public utilities. State of Connecticut. Retrieved from http://www.ct.gov/pura/lib/pura/electric/cyber_report_041414.pdf