



Government Technology Solutions

Experts Forum - California

Cyber-Security Funding in the Context of Homeland Security

February 10, 2005

Revised

By James J. Watkins

One area of Homeland Security that often gets neglected is Cyber-Security – making your data network safe from attack. Technology professionals are reluctant to admit to any deficiencies, since that would imply a sort of failure on their parts. Since they won't raise the issue, Executives and other financial decision makers tend to believe all is well, since "no news is good news."

The truth is every technology network is under constant attack from a variety of sources from malicious to merely inquisitive. And every network can benefit from an independent, "no fault" analysis of its security. This need not be – for starters – hiring a hacker for a complete "hostile penetration" test. Initially it's enough to do the equivalent of checking the doors and windows to make sure they're locked ... and that the key isn't under the mat. (Like continuing to use default settings and passwords for network administration.) Unless your network staff has been extremely diligent, dealing with the results of this analysis will keep them busy for months.

Here's a brief scope of work that would get the initial analysis done in 3 – 6 months, depending on the size of the network.

Network Architecture

- ❖ Review business requirements, objectives, and service levels
- ❖ Assess current backup systems, strategies, processes
- ❖ Recommend mechanisms for network status monitoring at staff and executive levels

Network Security

- ❖ Provide a high level analysis and assessment of current network security, internal and external
- ❖ Recommend areas for focus
- ❖ Provide a risk analysis and a strategy for risk reduction

A difficulty – especially in smaller jurisdictions and Special Districts – is an apparent lack of a funding source for an analysis like this. Well there is a source that may provide 100% of the costs, but getting funds will require considerable political (in the nice sense) skills. And there are a couple of cautions to go with it.

The federal Department of Homeland Security provides funds for specific projects, but not for personnel. So, you would need to contract out for the above scope of work. This year (Federal Fiscal Year 05), these funds are funneled through the California Office of Homeland Security. Specific guidance on how these funds may be spent is available through the website for the California Office of Emergency Services: www.oes.ca.gov.

<Continued

Federal guidelines are online at: <http://www.oip.gov/odp/docs/fyo5hsgp.pdf>

California-specific FFY 05 guidance is available at

<http://www.oes.ca.gov/Operational/OESHome.nsf/ALL/0B364D257932E8E088256F95006A3834?OpenDocument>

First, guidance from California's Strategic plan

- ❖ M.2 Assess the vulnerability of all critical infrastructure sites in California
- ❖ M.2a Conduct vulnerability assessments in conjunction with federal efforts.
- ❖ M.2b Coordinate vulnerability assessments with local agencies

Next from the Federal Grant Guidance itself

- ❖ Eligible activities include Developing and enhancing plans and protocols, including but not limited to:
 - ❖ Developing or enhancing cyber security plans
 - ❖ Developing or enhancing cyber risk mitigation plans
 - ❖ Developing public/private sector partnership emergency response, assessment, and resource sharing plans
 - ❖ Conducting point vulnerability assessments at critical infrastructure sites/key assets and develop remediation/security plans
 - ❖ Conducting cyber risk and vulnerability assessments

The basis for allocating funds is called "base plus population." The "base" part (\$20,000 for FFY 04) allows rural counties to get enough funding to do *some* projects. The "plus population" part allows the areas with the most people at risk to receive significant amounts of funding.

California distributes Homeland Security funding through the counties – called "Operational Areas" in the Emergency Services Act. An Operational Area is the boundaries of a county *and all the political subdivisions therein*.

Operational Areas must allocate funds as follows

- ❖ Fire services - 20%
- ❖ Police services - 20%
- ❖ Emergency medical services - 20%
- ❖ All other disciplines (discretionary) - 40%

This is where the political skills come in. Your request for funding will be ruled on by an Operational Area Council (whose composition varies from place to place), where it will be competing against first responder requests for "boots and suits," as well as "all other disciplines." Once the Council approves it, the funds are – almost! – all yours. The "almost" leads to the cautions I mentioned earlier.

The first cautionary note is that the funds are *reimbursed* after the expenditure. So a Special District must have enough "float" in its budget to cover the initial expenditure. Then you send an invoice to the state to get your money. Keep all documentation, including timesheets and receipts, for three years. You'll need it in case of an audit.

The second caution is that there are reporting requirements associated with the funds. The good news is that these quarterly report requirements can be easily met if you (a) have a project plan and (b) keep to it. Then you simply report on milestones achieved in accordance with the project plan.

The final caution is that the results of the analysis become available under the Public Records Act. It's important to know that once you have a report that lists vulnerabilities, a member of the public could ask for and get it. And that's another good reason to act quickly on the findings and reduce your vulnerability!

About the expert

James J. Watkins is President and CEO of JJ Watkins Consulting. He is the former CIO for the California Office of Emergency Services, where, among his other duties, he chaired the Cyber-Security Subcommittee of the California Statewide Strategic Committee on Terrorism. Mr. Watkins is an advisor to Government Technology Solutions on Cyber-Security Public Policy Issues.

916.947.0546

jim.watkins@comcast.net

This article will appear in the March 2005 edition of the California Special Districts Association newsletter

For more information contact us

Government Technology Solutions

4110 Business Drive, Suite A • Shingle Springs, CA 95682-7230

800.326.5683 • Fax 530.677.1416

www.gvTechSolutions.com