

[WP-016]

Whitepaper: Critical Infrastructure Visual Information Criteria [CIVIC]

Methodologies for Preventative Measures/Countermeasures to Safeguard CIP

Version 050113

January 2005

Author: Bob Radvanovsky, rsradvan@unixworks.com

(A special thanks goes to those listed for being my “sounding board” on this project.)

Copyright © 2005 Bob Radvanovsky. All rights reserved.



Limited Liability Statement

In no event shall the author(s) be liable for any found errors contained herein or for any direct, indirect, special, incidental or consequential damages (including lost profit or lost data) whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material.

The information contained within this document may be subject to change without any notice. No trademark, copyright, or patent licenses are expressly or implicitly granted (herein) with this whitepaper.

Documentation pertaining to any security-related technical or proprietary information, its data and all information provided and contained within this document is considered proprietary in nature and subject to copyright protection and is intended solely for use by its owner. Additionally, this documentation is solely for discussing a possible, and/or proposed critical infrastructure protection (CIP) security issues, and is not dependent upon any specified infrastructure, architectural condition or its issue(s). Source information is through observation from previous circumstances, related online documentation, and discussions with colleagues within the security field.

All other product names mentioned herein are trademarks or registered trademarks of their respective owners. NOTE: Any names not outlined or mentioned above are fictional in nature; as such, any relation to any name or trademark (if any) is purely coincidental.

Introduction

It has been said that our country is heading towards a sociological disaster of epic proportions insofar that we are willingly giving up our freedom, our rights, and our individuality in the name of “national security”. Fact is, the United States is one of the few remaining civilized countries throughout the world that hasn’t either retrofitted or replaced their infrastructures effectively that would reflect the quickly and constantly changing world. Another fact is that many of the various sectors that make up those identified and listed within former President Clinton’s PDD-63 Directive as “critical infrastructures”, lack many important functionalities and features that would (otherwise) provide and enable proactive measures – or even countermeasures – thus preventing (or in some cases, eliminating) further risk through investigations of physical attributed weaknesses of those various infrastructures.

So what exactly am I talking about?

On January, 2005, several online magazines announced that Hewlett-Packard and Phillips were introducing an encrypted version of the DVD that would render any future unauthorized duplication of DVD disks ineffective. According to these articles, devices introduced into the United States market after July 1, 2005 will have this technology built into the drives (burners and readers) and blank media. Ironically, the FCC has approved the introduction of the “broadcast flag” which would enable digital broadcasts of television, movies, radio – pretty much any type of multimedia – to be prohibitive from duplication.



Essentially (in simplified terms) the “broadcast flag” introduces additional data into the data stream to protect the digital rights of the broadcasted material (whether audio, video or both) from being copied or duplicated, such that having this flag enabled would render whatever device is attempting to record the multimedia being broadcasted useless. Basically, the device wouldn’t be rendered useless permanently, only temporarily or during the time that the “broadcast flag” were enabled; the effect would be temporarily until the broadcast subsided or was not enabled (such as public access radio or television where the likelihood of having the “broadcast flag” enabled would be significantly less than commercial, cable or satellite broadcasted materials. Through it is probably unknown what exactly would be shown at the time of the attempted recording, one might speculate that it would display an error or status message showing the ruling/reason for the temporary disablement.

How does this apply to “critical infrastructure”, and how would it be possible to have something similar to protect our “critical infrastructure” environments?

Actually, there is a solution that is rather simple.

Introducing the “Infrastructure Flag”

Our culture is quickly moving towards being completely and totally, a truly digital world. Case in point -- the recently introduced digital SLR cameras – demonstrates how our society is moving towards all digital and away from the traditional film-based cameras. Not that film will or may ever go away – many professional photographers that I know and have spoken with over the past several weeks/months have indicated that film-based technology won’t completely go away, but will significantly subside/wane, thus being left solely (or mostly) for the “professional photographer” in mind.

The technologies introduced years ago brought us the “digital camera” – a revolutionary device that allows consumers to take any type of photograph or video without any significant knowledge of photography at all – just point and click. The (then) newly introduced technology offer cameras that had 1 million pixel (called “megapixel”) imaging capabilities. Initially, you needed a bulky floppy disk or large memory stick, along with a media converter for a floppy drive or PCMCIA card slot (for laptops). Images were stored in common formats of TIFF or JPEG, and allowed consumers to immediately view their images as soon as they took them.

The “digital photography revolution” had begun!

What started out as 1 megapixel, then 2, shortly 3, then 3.4, then finally 4. At some point in time, it jumped to 11 and 12 megapixels, but this was limited (usually in the cost of the device) to “professionals only”, such as news media photographers. There was no such thing a 6 or 8 or 11 megapixels available for the consumer. Today, there is such a thing -- it is now available as a consumer-grade product. In 2003, Canon introduced the “digital SLR” camera called the “EOS 10D” – a 6.3 megapixel camera, capable of capturing near-photographic quality images. Initially, this camera was slow and cumbersome, but Canon



made improvements introducing a slightly faster, more robust version called the “Digital REBEL” (model “EOS 300D”).

For roughly \$1200, you can now have a complete camera kit (camera lens, body, and fast-cached flash memory stick) that is considered “professional grade” and provides a rather suitable resolution at 6.3 megapixels. The inference is that now anyone can acquire a professional grade camera that has a suitable resolution that can be used for reconnaissance purposes; that very camera can take hundreds of photo-quality images that can be enhanced, enlarged and encrypted. Those images may be easily sent away for analysis for further instigation.

By implementing a transmission station at the more critical locations of the various “critical infrastructures”, a transmitter can broadcast the “infrastructure flag” preventing anyone within a shortened radius of the location, from taking any picture or video for reconnaissance purposes. However, such an implementation is not without its drawbacks.

Drawback #1

The weakness of this premise is that 35mm film-based cameras will always be around. However, many camera manufacturers are slowly halting production of their film-based cameras and further enhancing/developing their digitally-based cameras. With a 35mm camera, and a decent zoom lens, just about anyone can take decent still images of whatever site are being targeted. I feel that, given in time that eventually, 35mm cameras will be cost-prohibitive such that people will rely solely upon digital devices for photography and video capture, which will be in about 20 maybe 30 years. That’s the first drawback.

Drawback #2

Those who live close or nearby to the critical location of the various “critical infrastructures” would have difficulty operating their own digital devices for “personal use”. This, obviously, would be the exception; however, in today’s world, esp. at the levels of paranoia that exist, would it be possible to make exceptions? Doing so could place whatever technological solution into place ineffective and render it useless. The risk associated with making such exceptions might encourage terrorist groups to target those nearby to a “critical infrastructure”, capture nearby residents, terrorize them, and then use their “imaging capabilities” to take reconnaissance photos or video before blowing it up, destroying it, or rendering it inoperative. Also, if an exception could not be given, those who would want to utilize such digital devices would have difficulty doing so, thus would cause some political upheavals with its citizens.

Drawback #3

Supposed that those who are in power do decide to elect to make exceptions to its implementation, then what? How would that be done? Basically, each and every device nearby to the critical location of that “critical infrastructure” would then be required to be “registered”; that is, the government would require that individuals would need to register their devices, either have a special code or key device entered or enabled within the digital device, then handed back to them. The stipulation would be that the device could never be sold, and would be near impossible to track or determine if someone were crafty enough with electronics. Essentially, this would require a significant undertaking by the government, imposing a high cost restriction on an already highly cost-prohibitive effort by the



government. Plain and simple of it is, it makes absolutely no sense to make exceptions. This again, would have a political impact upon the citizens.

Drawback #4

What about technological “glitches”? What would happen then? It comes down to that the more critical locations of the “critical infrastructures” would be constantly monitored 24x7 by cameras, video surveillance, motion sensors, etc. If there are any technical issues, they would be resolved in a shortened period of time, but may pose some problems to nearby residents.

Drawback #5

How would it be implemented? This would require a consortium between the manufacturers and the government, to implement technologies within each device such that the device would have a simple antenna (probably a small wire-based antenna within the housing of the device) that would render the device inoperative if removed or defective. The problem is convincing manufacturers of these devices to implement such a solution. Initially, the costs would be significantly high, but over an extended period of time, the cost could be minimized if implemented quickly.

How does the “Infrastructure Flag” work?

Similar to the “broadcast flag”, the “infrastructure flag” can be either analog or digital in its design. It requires a small antenna at each critical location of the “critical infrastructure” being visually protected, along with a small transponder (about 2 to 3 inches squared) which would operate at a low to very low frequency using a low wattage transmitter. This device would broadcast a pulsed beacon every 10 to 30 seconds. If the digital device “hears” the beacon, it is temporarily rendered inoperative, or displays an error or status message stating that it cannot perform the operation.

From a cost perspective, it’s rather simple. Each critical location would have 1 maybe 2 transponders, whereby each transponder kit would cost less than \$100 per unit cost. Power would be supplied by solar battery, so the need or dependency upon the electrical grid (caused by outages) would be minimized, thus eliminating the risk of electrical dependencies. However, with solar power, requires solar cells, which could cost more than \$100 for the unit cost, so perhaps battery-powered alternatives could be another method (meaning connect the devices to standard electrical sources, but have a significantly large battery backup supply for several days (if not weeks) if an electrical outage were to occur).

The transponder would be located atop of a wall of small structure, but not emplaced on any towered structure due to the fact of electrically discharged strikes from weather occurrences. Walls and small structures are usually grounded and are lower to the ground than tower-like structures, which just beckon to be struck by, lightning. With the transponder in place, with a small antenna (about 1-3 inches in height), on a low frequency using a low wattage (really low – say 0.1 watts of output power), can have an estimated effective radius of upwards of 1500 feet from the critical location of the “critical infrastructure”.



The devices can be protected by whatever security monitoring company would be monitoring the site, and if in the event the transponder fails, would dispatch a technician to either fix or (more than likely) replace the unit.

The device would be emplaced at critical locations such as: a nuclear power plant (this would require a transponder with a slightly higher wattage output due to the fact that the facility ground may encompass a much larger area), an energy substation, a gas transfer station (such as a fuel depot, or natural gas substation), “visually sensitive” areas such as loading docks or hidden entrances to buildings, etc. The possibilities are endless.

In conclusion, it is not surprising that within the next 30 years (if not sooner), it is conceivably possible that implementing such technologies may very well be possible, and perhaps, implemented. If there are such endeavors currently underway, I am aware of if they exist, and if not, I am not attempting to promote the implementation of such a technology. However, it is wise to note that in our increasingly growing paranoid world, such implementations will (eventually) happen.

