

Best Practices Make Perfection

(The Lost, the Misguided and the *Sintras*.)

May 2009



ON CYBER PATROL

As covered or mandated by AR 25-2



Information Assurance requires the practical combination of approved technology, adequate and appropriate training, understanding of all relevant rules and regulations and the common sense use of Best Business Practices (BBPs). “Best practices” is a common term used throughout the military, government and private sector that simply means the best way to do something. Army OIA&C adopted the use of this concept as an innovative approach to enforce standing policy while adjusting to the rapidly changing and emerging technologies. Unfortunately, there is one very common activity that makes BBPs all but useless. Some people do not follow them.

BBPs are developed collaboratively by the Army’s subject matter experts working with other leading organizations and subject matter experts. These experts ensure that published BBPs are the best way of performing a task using current knowledge, policy, and technology. Even then, there is no guarantee that a BBP will work when a new widget is invented or a better technique is discovered or if a situation is “unique”. That is why BBPs are living documents, adapting to emerging technologies, better processes, or enhanced standards. BBP sources should be checked on a regular basis to avoid falling behind the knowledge curve.

Yet, all the hard work that goes into BBPs and the valuable guidance they provide are lost if they are not used. The people who don’t use BBPs generally fall into one of three categories: the Lost, the Misguided and the *Sintras*.

The Lost are often new to a position with IA responsibilities and are not aware of the existence of the BBPs (See website above, top of left navigation bar.) Their jobs and their success in those jobs will be greatly improved by using these BBPs.

The Misguided are those that fall under the influence of the old timer in the office or unit that has “always done it like this.” Unfortunately, what worked yesterday make not work today in the fast paced IT world. New personnel look to seasoned coworkers and soldiers for advice. If you give advice, make sure it’s correct. Consult the published BBPs on a regular basis.

Finally, there’s the *Sintras*. Those are the people that always do things, as Frank sang it, “My Way.” These individuals present the greatest risk potential because they are so convinced their way is best that they won’t be swayed even in the face of a BBP’s proven effectiveness. Or if their way truly is better, they won’t share it with the Army community. Being individualistic is great. Causing, or not preventing, military data compromise via stubbornness or selfishness isn’t.

Avoid falling into one of these categories. BBPs are there for a reason. Highly qualified subject matter experts put a lot of effort into making sure that these valuable tools will help you get your IA job done right and often more easily.

(Addendum for all Army personnel)

The Army’s Office of Information Assurance and Compliance has an extensive list of IA BBPs that are available on the IA website (<https://informationassurance.army.mil>). This is a regularly updated resource for all Army personnel whose responsibilities at either the tactical or strategic level include IA functions. This can range from Data at Rest practices when they are on the road or Wireless Security Standards BBP. These BBPs act as the practical work day policies for IA. They are the best way to perform the covered IA functions and are not just a list of suggestions. They are the best methods known to work within the Army’s IT infrastructure. The BBP process is founded on leveraging the knowledge and expertise within the Army, and your expertise, standard, or best ideas can be submitted. Great ideas and standards are

often implemented and institutionalized at the lowest levels first and greatly enhance mission effectiveness and security. Without the ability to leverage lessons-learned and best practices in an active framework, then it all fails. As any IA person will tell you, any system not properly secured is a risk to all of the Army and DOD. Any compromise jeopardizes millions of users and systems, often with just one click of a mouse.