NSASB FRG Training

Code of Conduct

&

OPSEC

As of 7 Jun 2017

Code of Conduct

- All members of the NSASB Family Readiness group are expected to present themselves in a professional and courteous manner at all events. When you represent the FRG to others, you represent the Command.
- Members of the NSASB FRG must follow the law, act with integrity and honesty in all matters, and be accountable for our actions. The TEAM SOUDA family represent the U.S. to our Host Nation.
- Understand and follow OPSEC policies…the safety of NSASB, our visitors, and the ability to perform our mission depends on it.

- The following will NOT be tolerated and may result in resolution through the Conduct Review Board:

- Abuse of any kind against another member at NSASB FRG events or in any social forum.
  - This includes but is not limited to sexual, physical, emotional, and verbal.
- Intimidation, threats, or retaliation against another NSASB FRG member.
- Making false accusations against members.
- Falsification of any NSASB FRG document.
- Violation of current the by-laws.
- Violation of the NSASB FRG Standing Rules.
- Breaches of personal information

Operations Security

- **Operations Security (OPSEC) is a process that identifies unclassified critical information (CI), outlines potential threats and the risks associated and develops countermeasures to safeguard critical information.**

- **Success of operations depends on protection of CI.**

- **Capabilities and intentions of an adversary to undertake any action detrimental to the success of friendly activities or operations.**
  - Conventional Threats
    - Military opponents
  - Unconventional Threats
    - Terrorism (foreign and domestic)
    - Hackers
    - Insiders (Spies)
    - Thieves, stalkers, pedophiles

What are they looking for?

- **Names, photographs of important people**
- **Present/future operations**
- **Information about military facilities:**
  - Location
  - Number of personnel
  - Ammo depot locations
  - Dates and times of operations
- **Family details**
  - Spouse, children
  - Location of work, school

Critical Information

- **Information we must protect to ensure success**
- **Information the adversary needs to prevent our success**
  - Capabilities
  - Operations
  - Personnel
  - Security procedures

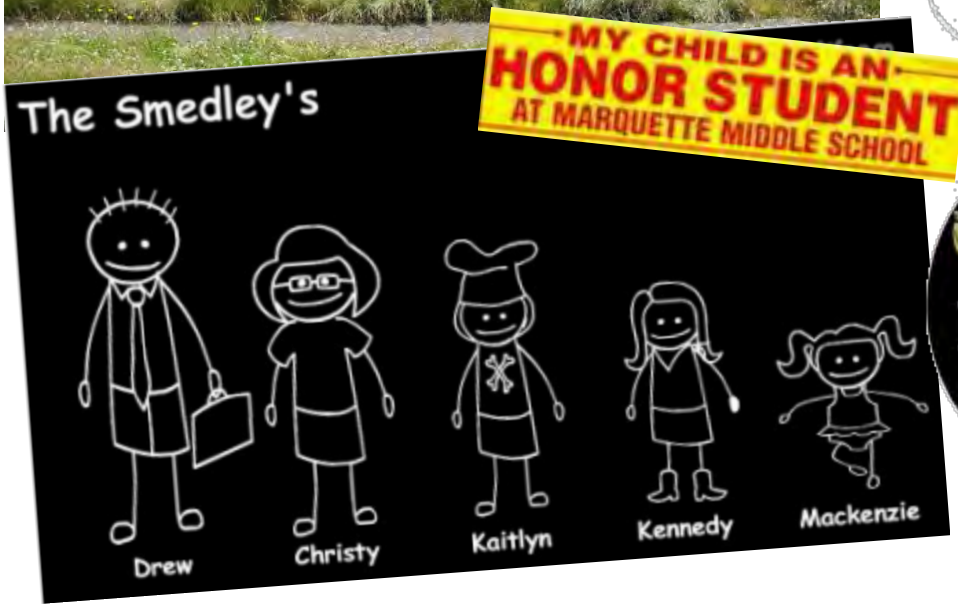
Geotagging

- **GPS data embedded into photos**
- **Default feature in most smart phones and digital cameras**
  - Latitude/longitude
  - Device information
- **Information can potentially be retrieved from any photo posted on the Internet**

- **Friendly, detectable actions that reveal critical information and vulnerabilities**
  - Longer working hours
  - Rehearsals
  - Sudden changes in procedures
  - Onloads
  - Large troop movements
  - Emblems/logos
  - Routine predictable procedures

- **Not all indicators are bad**

Avoid Indicators



Vulnerabilities

- **Weakness the adversary can exploit to get CI**
- **Some common vulnerabilities are:**
  - Lack of awareness
  - Social media
  - Social engineering
  - Data aggregation
  - Technology
  - Trash
  - Poor policy enforcement
  - Unsecure communications
  - Predictable actions/patterns

Countermeasures

- **Anything that effectively negates or reduces an adversary's ability to exploit vulnerabilities or collect & process critical information**
  - Hide/control indicators
  - Vary routes
  - Modify everyday schedules
- **Influence or manipulate an adversary's perception**
  - Take no action
  - React too late
  - Take the wrong action

OPSEC in Social Networking

- **What do you display in your social networking profiles?**
  - Where you work
  - Where you are
  - Where you have been
  - What you are doing right now
  - Everything that you have done
  - What you like and don't like
  - Your birthday
  - Your favorite pet
  - Your relationships
  - Your loved ones
  - The people you trust

Facebook
Terms of Service Agreement

- "…you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide **license to use any IP content that you post on or in connection with Facebook** (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it."
- "When you publish content or information using the Public setting, it means that **you are allowing everyone, including people off of Facebook, to access and use that information**, **and to associate it with you** (i.e., your name and profile picture)."
- "**You give us permission to use your name, profile picture, content, and information in connection with commercial, sponsored, or related content** (such as a brand you like) served or enhanced by us. This means, for example, that you permit a business or other entity to pay us to display your name and/or profile picture with your content or information, **without any compensation to you**. If you have selected a specific audience for your content or information, we will respect your choice when we use it."

Facebook Data Policy

- “We collect the content and other information you provide when you use our Services, including when you sign up for an account, create or share, and message or communicate with others. This can include **information in or about the content you provide, such as the location of a photo** or the date a file was created. We also collect information about how you use our Services, such as the types of content you view or engage with or the frequency and duration of your activities.”
- “We collect **information about the people and groups you are connected to and how you interact with them**, such as the people you communicate with the most or the groups you like to share with.”
- “We collect information **when you visit or use third-party websites** and apps that use our Services”
- “Keep in mind that **information that others have shared about you is not part of your account** and will not be deleted when you delete your account.”
- “We may **access, preserve and share your information in response to a legal request** (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may **include responding to legal requests from jurisdictions outside of the United States**…We may also access, preserve and share information when we have a good faith belief it is necessary to: detect, prevent and address fraud and other illegal activity; to protect ourselves, you and others, including as part of investigations; or to prevent death or imminent bodily harm.”