Testimony of Erik Kleinsmith to the joint hearing of the
Terrorism, Unconventional Threats and Capabilities Subcommittee and
the Strategic Forces Subcommittee on Armed Service
on the Able Danger Project,
15 February 2006

Good afternoon Mr. Chairman and members of both subcommittees. Thank you for inviting me to testify about my involvement in the Able Danger Program today. I have been asked specifically talk about my role in an open session with the understanding that I may be invited to return and answer your questions in a closed session later.

When US Special Operations Command or SOCOM requested support in January of 2000 from what was then called the Land Information Warfare Activity or LIWA, I was the Chief of Intelligence of that organization in charge of 24 personnel including officers, soldiers, and civilian intelligence analysts. My branch's primary mission was to provide intelligence support to LIWA for information operations that included Army and Joint deception, psychological, and information security operations. To do this, my branch conducted analysis on a wide array of threats ranging from foreign based hacker groups to terrorist networks and other asymmetric threats.

What is important to understand in relationship to the Able Danger program is that LIWA, now called the 1st Information Operations Command or 1st IO, was not an intelligence unit. It was an operational unit and as such was only part of the Intelligence Community as a subordinate unit of the US Army Intelligence and Security Command or INSCOM. My branch within LIWA was not a recognized national intelligence producer in the same way that organizations like DIA or NSA are considered. What made the distinction between LIWA's operations and traditional intelligence operations even more blurry was our co-location at INSCOM's Headquarters on Fort Belvoir, Virginia. My intelligence branch was part of this operational unit much in the same way that any combat unit has intelligence personnel supporting it on the battlefield.

While my branch was unique in terms of the types of analysis that we did, we were even more so because of the capabilities available to us in our Information Dominance Center or IDC. The

IDC was and is not a unit or a particular software tool, but a physical center owned by INSCOM and maintained by LIWA, again, now 1st IO. Working in the IDC, my analysts had access to state of the art data mining and visualization tools far above what a majority of the rest of the Intelligence Community had available at that time. My analysts and I could harvest and visualize huge amounts of structured and unstructured data on a daily basis. For example, instead of surfing through raw information or reading intelligence reports one message at a time, we could visualize thousands of messages simultaneously and through proper analysis, identify the key entities and their relationships or "linkages" to one another. My branch could conduct preliminary analysis in a matter of hours on information that might take more traditional analysts weeks to manually plow through

Because of our abilities, our support was routinely requested by several customers that took our work far outside our normal mission of supporting Army information operations. In the two years that I was Chief of Intelligence, we provided analytical support to every Combatant Command and several times I notified my chain of command that my analysts were overwhelmed with tasks. Because of our ability to understand data mining technology from an intelligence analytical perspective, Dr. Eileen Preisser and I spent a lot of our time inventing new and rewriting traditional analytical processes that gave my analysts even better ability to take advantage of the IDC tools.

Coordination for our support to SOCOM's Able Danger Project began in December of 1999. After an assessment of our capabilities in comparison to other intelligence organizations, SOCOM requested our support in January of 2000. By February we were conducting massive data mining and analysis of al Qaeda and other terrorist groups associated with that network. I would like to stress that during this time my branch was completely supported by my chain of command that included the Commander of LIWA, Colonel Jim Gibbons, and the Commander of INSCOM, then Major General Robert Noonan.

One of the pivotal questions that has come up since 9/11 is whether or not Mohammed Atta or any of the other hijackers were identified by an infamous chart produced during this time. I reiterate my answer that I gave to the Senate Judiciary Committee that I do not remember seeing Mohammed Atta's name or face on a single specific chart. The more important point is that our

team was tracking hundreds of names and creating dozens of charts for SOCOM. And while most of these charts contained information and intelligence that needed further analytical vetting, we were still able to identify a significant worldwide footprint with a surprisingly large presence within the United States.

In the middle of our preliminary analysis of the data, we were ordered to cease our support to SOCOM due to what we were told were intelligence oversight concerns. While I received the order through my chain of command, we knew that the order had come from somewhere in the Pentagon. Even today neither I, nor any of the other team members that I have spoken with, can say exactly where the order originated. This order, along with a subsequent six month struggle for LIWA and INSCOM to get permission to restart our work was a huge source of frustration felt by both our team and our SOCOM contacts. SOCOM finally grew so impatient with our inability to overcome our work stoppage that they decided to move their analytical operation to a Raytheon facility at Garland, Texas and continue their own efforts without our support. By the time we were allowed to begin work again, the bombing of the USS Cole had changed the face of our entire effort completely.

It was during this work stoppage around May of 2000 that I was required to delete all of the raw information, data, and products that we had collected and developed during our support of Able Danger. I was required to do this to comply with intelligence oversight regulations covering incidental collection of data on US persons. These regulations dictated that information on US persons could be held for only 90 days without a further determination of the validity of the information. In using data mining tools, we had to assume that there was information on US persons throughout all of our datasets. Since we were barred from working with any of the data for either analysis or vetting of US persons, it all had to go when the 90 days were up.

I thank you again for the opportunity to appear before you and am happy to answer any questions that you may have.