MODULE 1 - WHERE ARE WE?

LECTURE 7 - This lecture introduces the acronyms CUISC, KISS and CUIPDSC

CUISC & KISS – WHAT ARE THEY?

The traditional investigation process for Visible crimes can be described as the **COLLECTION** and **USE** of **INFORMATION** to **SOLVE CRIME**. To facilitate things, the acronym that we'll use for this is **CUISC, C-U-I-S-C**.[14, 16, 17, 18] This is essentially me applying the **KISS** principle, OK? So I'm going to avoid getting too technical with any detailed parsing of words or meanings. I just want something easy to remember that I can work with, and that you can **REMEMBER!!** So we're gonna go through each letter of the CUISC acronym and explain what the words that the letters stand for mean.

- C is for COLLECTION. This relates to the interface between the police and the public – how the police recognize, detect, identify and **obtain, or collect,** crime-related information.

- U refers to the USE of information, or how police **use** it within the criminal justice (CJ) system – how it is organized, analyzed, processed, stored and retrieved.

- I is for INFORMATION. This is broadly defined **as opinions, facts, and/or data**, the source of which is either people or things. But because information is a **concept**, it cannot do anything by itself. It **requires people** to collect, to put it in their head, and then to use it. You **remember** that, right?

- S is for SOLVE, which means activities ranging from the informal discretionary **disposition** and/or dismissal of complaints, to the full investigation and subsequent prosecution and conviction of offenders.

- C is for CRIME, which is **human behaviors**, usually categorized as felonies, misdemeanors and lesser violations, which are defined by the CJ system, and for which the CJ system provides formally sanctioned punishment. In this course we're using the five major categories of crime, which I described before.

So as I said earlier (the **KISS** principle), we can haggle over these definitions, and sometimes that's really important and worthwhile to do. But for our present purposes in this course, we will apply them in a generally practical way in order to make broader points and address other issues. And if we come up with any

particularly glaring problems, we can always take a little time to address them to the point where we can move on again. Or we can just ignore them, OK?

Now with regard to the terms **COLLECTION and USE,** I need to mention a few things. And yes, some of them are repetitious.

COLLECT INFO FROM PEOPLE & THINGS

The two main sources of crime info are **People** and **Things** (recall the theoretical perspective stuff we covered earlier):

- People (including Victims, Witnesses, Informants and Subjects) are by far the **primary source** of crime info for the police. Always have been, and always will be – as we'll see in later lectures.

- Only people can **recall** past behaviors (such as crimes), and **connect** things (memories, physical evidence, info systems, etc.) to past behaviors.

- The police/public **relationship is critical** to collecting info. Depending on how well the people and the police get along can affect the quality and quantity of crime info reported to and collected by police.

- Fewer than half of all Visible NCVS violent crimes, and **one-third** of NCVS property crimes committed in the US are reported to police. That means **close to 2/3 are not reported**. And that's what the **victims tell us**. This raises some **question** about the police/public relationship. **Ya think**?

- **Less than 5%** of the Index crimes are discovered by the police themselves. 5%? **Criminetti!**

(Reference 139, BJS, 1988: "Police are the first to discover crime in 2.5% of all reported crimes." (p35). "Police discover 3% of reported personal crimes and 2% of reported household crimes." (p 62).

- Therefore, the police/public relationship eliminates almost 2/3 of NCVS-tracked crimes (which are generally comparable to UCR Index crimes) from being reported to the police. This is essentially the **largest filter** of crime information entering into the CJ system. After 200 empires.

Common problems with **people** as crime info sources include, but are not limited to, legal issues (such as rights, protection, and confidentiality), reliability (including mental/drug/alcohol-related issues, accuracy of

info, false info, and corroboration of info), fear of police, self-incrimination, and people as potential suspects. And these are our **best** sources of info! Yes, CHAGRINED TRAVELER, sad but true.

The **second main source** of crime information is **things** – or physical evidence. Physical evidence includes things that are real (guns, fingerprints, body fluids, etc.). You can usually touch them, and they are artifacts of crime.

- Physical evidence is collected in **less than 10%** of Index crimes. **Remember** that?

- Most agencies do not have evidence technicians (specialists trained to collect and handle physical evidence). Not like on TV.

- The **most frequently collected** kinds of physical evidence are firearms, fingerprints, blood, hair and semen. **Yuck!**

- Most physical evidence is never submitted for analysis. Why? Because it generally does not identify offenders by itself (excluding ID cards, driver's licenses and such), and no suspects were developed during the investigation for comparison to see if it matched. DNA and fingerprints may be an exception to this – if they are found, recovered and in sufficiently good condition to permit analysis, and then if matches can be found in other information data bases. Oh yeah, **can do easy.**

Common problems with physical evidence include proper collection and preservation (to avoid contamination), maintaining control (to avoid tampering), the integrity of the evidence itself (sufficient for identification), and property identification (it can be difficult to establish specific ownership of most property). **Troublesome!**

Because physical evidence is collected and analyzed in so few cases, it generally plays only a **minor role** in investigations (despite what you may see on TV!). However, if and when it is collected, it **can be a valuable part** of the investigation, and it can also play an **important role in the interrogation, prosecution** and **sentencing** of offenders.

THE SHERLOCK HOLMES OF FRANCE

I want to take a moment here to talk about **Locard – that's L-O-C-A-R-D.** "What's a Locard?" you may ask. Well….

Quote, "Dr. **Edmond Locard** (born 13 December 1877, died 4 May 1966) was a pioneer in forensic science who became known as the "Sherlock Holmes of France." Unquote
In 1910, in France, Dr. Locard created one of the first police crime labs to examine physical evidence in order to link it to a crime. His basic idea was that **no matter where we go or what we do, we leave some sort of trace evidence, or some physical artifact of our behavior.** If we can detect this evidence, we may be able to use it forensically (in a court of law).

He formulated the basic principle of forensic science, which is:

"Every contact leaves a trace."

By that he meant, and again I quote: "…wherever he touches, whatever he leaves, even without consciousness, will serve as a silent witness against him… …his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value." Unquote. [54] Taken from Dr. Edmond Locard, 1942, "Criminal Investigation: Physical Evidence and the Police Laboratory," and published by Interscience Publishers in New York.

This became known as **Locard's Exchange Principle.** [54]

This is what I call a **brilliant insight**, and is essentially the basis upon which most crime labs operate today, as we shall see next.

<u>USE INFO FROM THINGS – LABS & DATA BASES</u>

Now I'm gonna talk about USE. That's the U part of CUISC.

There are many ways that crime information is used in investigations. Aside from how it is used in the Screening and Assignment process and by detectives, we focus here on **information systems.** These can range from telephone books and cell phones to crime labs and computerized data bases.

I like to think of information systems as essentially **containers** for info.

A **notebook** or a **telephone book** is a container of info. It stores info and typically organizes it in a specific way to facilitate retrieval.

A **cell phone or computer** is a container that can store, organize and facilitate retrieval of much larger amounts of info, and it can do so faster, and also allow for the manipulation of info.

A **crime lab** is a place where info in info containers can be identified, described, understood, manipulated (you **remember** IDUM, don't you?), tested, etc., with sophisticated tools and equipment in a rigorous scientific way.

So by using different types of info systems, we can increase the availability and use of information in criminal investigations.

So notebooks and cell phones and such are generally more for **individual** usage. But now we're gonna take a look at crime labs and large data bases, which are generally more **technically complex** and controlled by **organizations** rather than individuals.

Crime labs. There are more than 350 accredited crime labs in the US. [19]

- About 2/3 of all lab **workloads** is drug and alcohol analysis.

- The most frequently requested **analyses** are to identify controlled substances, toxicology and latent prints.

- Only about 120 crime labs in the U.S. can process **DNA** evidence. [20]

- The **three main purposes** of crime lab analysis are (1) to identify and classify evidence; (2) to associate evidence with a suspect; and (3) to exculpate (which means eliminate a person as a suspect).

Common problems include proper certification of lab procedures and personnel, quality control, testing standards, timeliness, overwhelming workloads, costs and priorities.

However, as technology improves and the field of forensic science develops at an increasingly rapid pace, the **advances** made in evidence collection and analysis in labs are literally **mind-boggling** in their ability to provide investigators with crime information.

Now I'm gonna talk about **Data Bases.** Some examples of large computerized crime information systems data bases are as follows: [21]

- NCIC (acronym for National Crime information Center) – this is a national computerized index of criminal justice information (i.e.- criminal record history information, fugitives, stolen properties, missing persons). This is a big one.

- AFIS (Automated Fingerprint Identification System) – this is the national fingerprint identification data base. You may be in this one if you ever had your fingerprints taken~~

- CODIS (Combined DNA Index System) – contains DNA profiles from crime scenes and of offenders.

These are **national-level** computerized crime data systems that most local, state and federal agencies have access to. They're all run by the **FBI**. Google them if you want to learn more about them. They're **awesome!!**

Common problems with these systems include technology (reliability, security, compatibility, outdated systems), information (GIGO, or garbage in, garbage out; reliability, currency, etc.), types and extent of access between agencies, quality controls, protection, protocols, etc. - you **name 'em.** Well, nothing's perfect.

Despite the myriad of problems, these systems are **massive repositories** for crime information that has already been processed at least to some extent by the CJ system. They serve as memory banks that grow larger over time by continuously documenting new crime information, organizing and storing it, and making it retrievable and available to agencies country-wide. This is a relatively new thing in our CJ system – pretty neat

and pretty powerful (heh-heh, chuckles the Government Spy!! We'll cover the Government Spy in the next module. In the meantime, just **enjoy these sneaky chuckles**).

So almost all agencies can now access new and old information about crimes and offenders all over the country and going back several decades in time. **Even Superman can't do that.**

So the police have to **play by the rules** we give them. They can improve their efficiency and effectiveness, but we tell them that they have to stay within the rules, especially when it comes to people (the **ol'** CC vs. DP stuff).

So now here comes **technology,** and it says that it can do things in **labs** to develop crime information and even identify offenders today in ways that were impossible to do just a few years ago.

And technology also gives police **national data bases** that are memory extenders that preserve and make quickly available to agencies tons of information about crimes and offenders that go back decades. (**Heh**-heh-heh!)

So things, specifically in the form of crime labs and national data bases, are rapidly providing all agencies much greater and faster access to crime information, both new and old, than they ever had before, or even dreamt of. Even though the info may have existed elsewhere in the CJ system or in people's memories, the operative term here is **ACCESS**! (**Heh**-heh, yeah, "access"~ I love access!). Police are gaining much greater access to all types of crime information, which includes all kinds of information about people.

So now the police are gradually learning to take **greater advantage** of the wealth of crime information that these "things" sources can provide. (**Heh-**heh, yeah, "greater advantage"~ That's good, too!)

However, the full extent to which these resources have influenced criminal investigations and improved investigative outcomes (or clearances) has **not yet been well-documented** in the research literature beyond anecdotal evidence.

So the police may be limited in what they can do with **people** as information sources, but a vast new area of information is opening up to them regarding **things.** Sounds like a real winner – but don't you think we will be

placing more and more **constraints** on them, too? I mean, shouldn't we constrain the police, even though crime costs us one trillion bucks a year, every year? Isn't our privacy worth it?

CUIPDSC – WHAT'S THAT & HOW DO YOU PRONOUNCE IT?

Before we continue further, let's just take a quick look at what happens with **the other four major** crime categories.

Well, first off, they are generally **not reported** to the police due to their nature (you can refer back to their definitions, discussed, earlier, if you can't figure out why), so police will likely never know about most of them. No crime labs or data bases for them, **eh?**

But the economic and social costs of these crimes are so great that the police often have to approach at least some of them a bit **differently**. The traditional investigation process just won't hack it. For these crimes, the police have to:

COLLECT and
USE
INFORMATION to
PREVENT, DETECT and SOLVE CRIME
The acronym for this is C-U-I-P-D-S-C, or CUIPDSC. [17] Man, this is as easy as eating pumpkin pie!

Unfortunately, those added words – **PREVENT** and **DETECT** – require a bit more than the traditional investigation process can muster. And, unfortunately, they can also be fraught with **problem-o's (heh**-heh), some of which we'll address later. But for now we'll just stick to talking about Visible crimes and CUISC.[6, 12, 13, 22, 23, 24, 25]

OK, INDEFATIGABLE TRAVELER, that's about it for this lecture. And that's enough, eh?