Warren County · Ohio
TELECOMatters
July 2017
our monthly newsletter of things that matter. all things Telecom.
for Public Safety

Radio Etiquette When Speaking to Dispatch

- Make sure there is no back & forth between another unit and dispatch before you begin your transmission. Let the unit complete their dialogue with dispatch before you begin.
  - Inquiry is the main check-in/check-out talkgroup for probation officers and dog warden but it's also where police submit license plates/SOCs/LEADS requests to dispatch so it can get busy at times.
  - PD Prim 1 is northern law agencies
  - PD Prim 2 is southern law agencies (Mason, Hamilton Twp, Maineville, So Leb & DF WCSO)
  - Fire Primary is shared by all Warren County-dispatched Fire/EMS agencies
- If Dispatch tells you to standby, that means to wait while they finish a conversation with another unit. They'll call for you when ready to receive your traffic.
- Some units are reportedly using different alpha-phonetics than Dispatch. The appropriate A-Z are shown right.

Consistent and courteous radio usage better insures your safety and organized communication with Dispatch. We pride ourselves on offering you state-of-the-art radios with the latest technology and superior communication ability. Part of that means the users operate the radio to the best of their ability!

Telecom offers a 90-minute radio refresher class for individuals, small groups, or entire departments! Contact our Community Manager / Trainer noted below to schedule your agency.

A – ADAM
B – BAKER
C – CHARLES
D – DAVID
E – EDWARD
F – FRANK
G – GEORGE
H – HENRY
I – IDA
J – JOHN
K – KING
L – LINCOLN
M – MARY
N – NORA
O – OCEAN
P – PAUL
Q – QUEEN
R – ROBERT
S – SAM
T – TOM
U - UNION
V – VICTOR
W – WILLIAM
X – XRAY
Y – YOUNG
Z - ZEBRA

Director 695-1318 paul.kindell@wcoh.net | CAD/RMS 695-2800 paul.bernard@wcoh.net | Data Systems 695-3250 jeff.cepin@wcoh.net
Radio Systems 695-2860 gary.hardwick@wcoh.net | Telephony 695-1320 garrett.wilson@wcoh.net | Training 695-2802 allison.lyons@wcoh.net

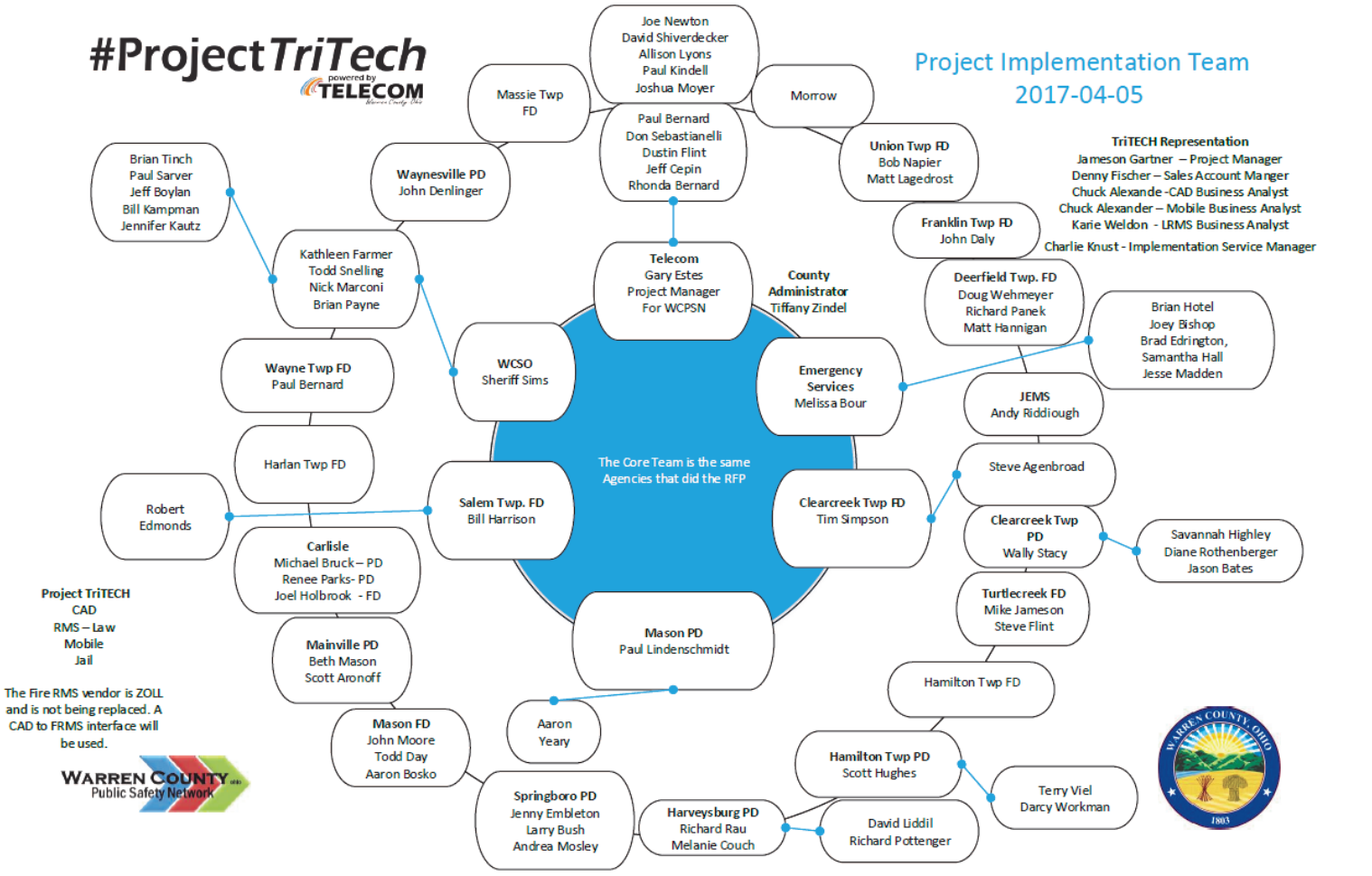
#ProjectTriTech

powered by TELECOM Warren County · Ohio

FOLLOW #Project*TriTech* on our Facebook/ Twitter + our 'Projects + WorkGroups' webpage

One-on-One Department Meetings Telecom will be reaching out to each Chief or their appointed decision maker to review and discuss an Agency Readiness Document. Its purpose is to walk each agency through the feature sets of TriTech and sign off on each of them. This will ensure all participants are on the same page moving forward.

Up Next: July 11-13 = Jail Workshop at Telecom's Training Room



Director 695-1318 paul.kindell@wcoh.net | CAD/RMS 695-2800 paul.bernard@wcoh.net | Data Systems 695-1810 gary.estes@wcoh.net
Radio Systems 695-2860 gary.hardwick@wcoh.net | Telephony 695-1320 garrett.wilson@wcoh.net | Training 695-2802 allison.lyons@wcoh.net

Help Us Gather Complex/Suite Address Points For TriTech

We need agency help in collecting ADDRESS POINTS for multi-site locations such as apartments, mobile home parks, business suites, and camp sites.

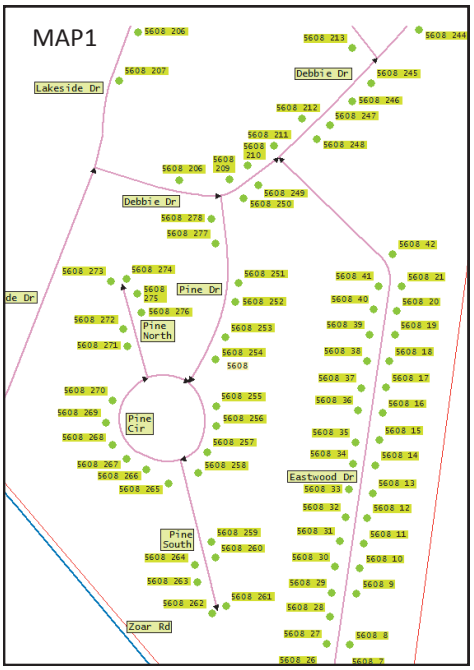
We are using 'phantom' streets on the map to allow TriTech CAD to route units directly to the reported address of the Call for Service. These are labeled Driveway, Parking Lot, or Access Road. Currently these have a speed limit of 20 mph so they will not be favored by the routing software. Crossovers are also being created with a speed limit of 5 mph.

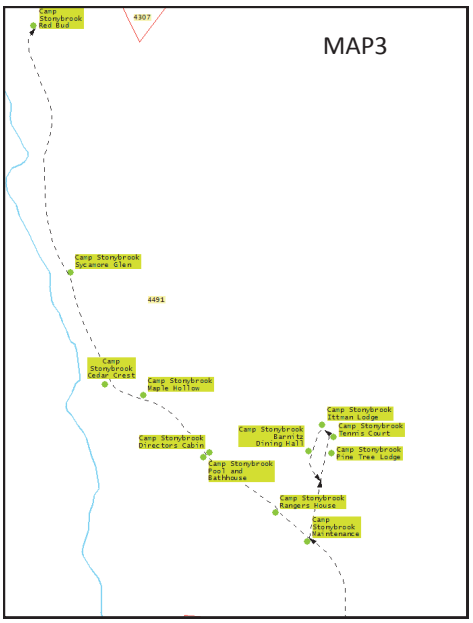
Map 1 shows Joy Acres Mobile Home Park in Hamilton Twp. An address point is on each lot along with th private streets and their names.

Map 2 shows a shopping center in Springboro. There are address points along the front of the building near the entrances. There are several possible routes available through the Center depending on from where the unit is responding.

Map 3 is Camp Stoneybrook. Even though it is all one address, the address points are used to locate features of the Camp such as lodges and cabins.

All features and their settings are easily changed and can be fine-tuned over time.





Since TriTech has mobile mapping, this data will be available on your MDC so the more you help us populate these locations, the more info you'll have at your fingertips (literally).

Changes in 2017 OIBRS Data Specifications

Data Element #17: Type of Criminal Activity

When a criminal report is entered into FBR or RMS and an offense is entered, one of the state mandated entries include criminal activity. This entry can currently be found in FBR under *offense detail* or in LRMS under the cover-sheet and statute.

Any report can have up to three entries for each listed statute. Statutes that must have the criminal activity completed are *gambling equipment violations, weapon law violations, pornography/obscene material, counterfeiting/ forgery, drug/narcotic offenses, drug equipment violations and stolen property offenses*.

Gang Codes: even if a gang is not involved, codes have to be entered for *murder/non-negligent manslaughter, negligent homicide, kidnapping/ abduction, assault offenses, sex offenses and robbery.*

New entries for Criminal Activity will be added into the new RMS system. The codes will include *simple/gross neglect, organized abuse, intentional abuse and torture, and animal sexual abuse* as possible entries bestiality).

TENTATIVE PAGING OUTAGE

Monday July 17th FROM 10-11am. Paging will be offline. Dispatch will drop an all-call and agencies will have to listen to portables for calls for service. We'll update via email and social media. We're adding paging at Blackhawk, Lytle, ODOT, and Wilmington Rd towers for additional paging coverage and power in these areas.

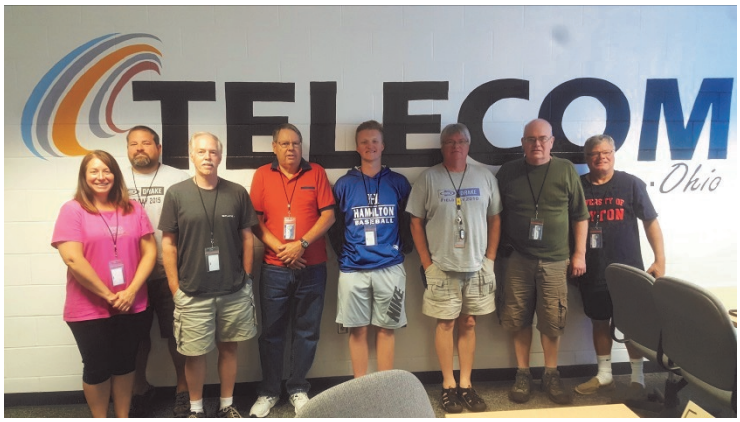
Coast Guard Aux Receives Warren County Radios

Interoperability is smoother with another federal agency now that the United States Coast Guard Auxiliary has (3) portable radios. When responding to Caesar Creek they can speak directly to our Fire/EMS and police agencies also on the scene. Further, on June 17th our Public Safety Systems Manager, Paul Bernard trained the Coast Guard staff on how things are done in Warren County's radio world.

NIFOG: Say "VFIRE21," not "Fire Mutual Aid," when referring to the VHF state wide fire mutual aid channel. This is a nationwide standard and Warren County units are reportedly calling it the wrong thing. Note: this is the frequency that can be used if you only have VHF or if 8TAC92D and 8TAC94D are unavailable for some reason.

Drake Radio Club at Telecom & Emergency Services

On June 23rd, the club, whose members includes our very own Radio Supervisor, Glenn McKeehan, received a tour and a lesson in how technology is used for Public Safety.



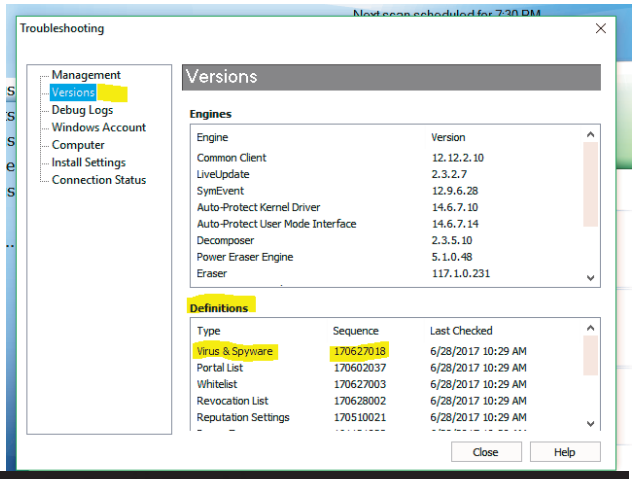
We at Telecom take your online safety seriously… protecting you and the many communities we serve. One of many steps we take is monitoring and quarantining your MDC to ensure we are always staying within safe levels of online security. We appreciate your continued efforts to stay within these safe levels of service. Please contact us if you have any needs or questions. Thank you from all of us here at WC Telecom!

Petya ransomware outbreak: Here's what you need to know

By: Symantec Security Response 27 Jun 2017

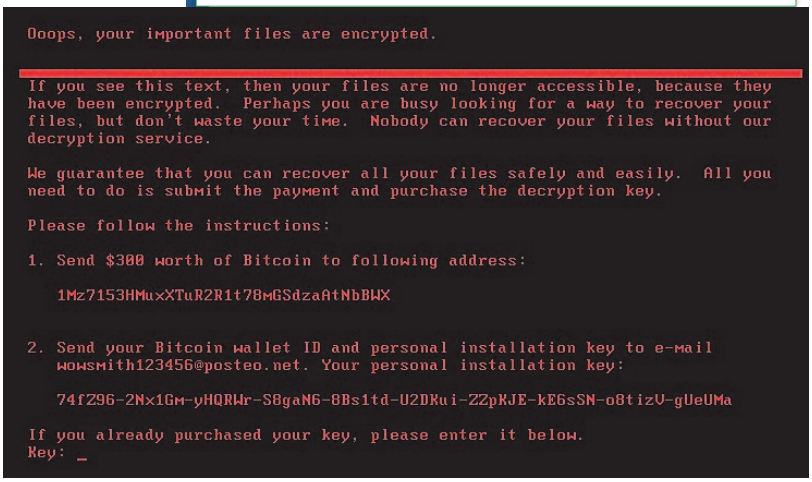
A new strain of the Petya ransomware started propagating on June 27, 2017, infecting many organizations. Similar to WannaCry, Petya uses the Eternal Blue exploit as one of the means to propagate itself.

Am I protected from the Petya Ransomware? Symantec Endpoint Protection (SEP) and Norton products proactively protect customers against attempts to spread Petya using Eternal Blue. SONAR behavior detection technology also proactively protects against Petya infections. Symantec products using definitions version 20170627.009 also detect Petya components as Ransom.Petya. As seen in picture below we are at .018 as of 6/28/17



What is Petya? Petya has been in existence since 2016. It differs from typical ransomware as it doesn't just encrypt files, it also overwrites and encrypts the master boot record (MBR). In this latest attack, the following ransom note is displayed on infected machines, demanding that $300 in bitcoins be paid to recover files:

Figure. Ransom note displayed on computers infected with the Petya ransomware, demanding $300 in bitcoins



How does Petya spread and infect computers? One of the methods Petya uses to propagate itself is by exploiting the MS17-010 vulnerability (Security Update for Microsoft Windows SMB Server (4013389)), also known as Eternal Blue. Symantec continues to investigate other possible methods of propagation.

Who is impacted? At the time of writing, Petya is primarily impacting organizations in Europe.

Is this a targeted attack? It's unclear at this time, however, previous strains of Petya have been used in targeted attacks against organizations.

What are the details of Symantec's protection? Network-based protection: Symantec has the following IPS protection in place to protect customers against these attacks:

OS Attack: Microsoft SMB MS17-010 Disclosure Attempt (released May 2, 2017)

Attack: Shellcode Download Activity (released April 24, 2017)

Attack: SMB Double Pulsar Ping Web Attack: Shellcode Download Activity 4

Antivirus Ransom.Petya Ransom.Petya!g1

SONAR behavior detection technology SONAR.Module!gen3

Symantec is continuing to analyze this threat and will post further information as soon as it becomes available.