May 2017



Inside this issue:

1
3
3
3
4
4
5
5
6
6
7
8

The Next OCRACES Meeting Is

May 1, 2017 1930 Hours

840 N. Eckhoff St., Suite 104, in Orange

Presentation by Brenda Emrick, Kl6EXL, Costa Mesa Fire Dept.



Orange County Sheriff's Department Communications & Technology Division



Newsletter of the County of Orange Radio Amateur Civil Emergency Service

Captain's Corner by RACES Captain Ken Bourne, W6HK, Chief Radio Officer

Cyber Attack

Recently I received e-mails supposedly from a couple of City RACES Chief Radio Officers and from other friends, with no comment but just a link to a Web site. I say "supposedly," because those e-mails were really not from my friends but, rather, were from cyber criminals posing as someone I knew. If I had clicked on the links, I would most likely have been directed to a Web site that would have infected my computer with malware, a virus, or, worst of all, ransomware. The e-mails I received were either from my friends' infected computers sending e-mails to their e-mail client's address book, or directly from the bad guys who had hacked into my friends' e-mail accounts. The moral of the story is: Do not click on a link in an e-mail message from a friend or from an unknown source, especially if there is no convincing statement in the e-mail that the link and source are legitimate. Furthermore, if you receive a suspicious link from a friend (including me!), tell your friend about it. If he denies he sent it, he should then run a virus scan on his computer, or check to see if his e-mail account has been hacked. If someone reports that he received a "bad" e-mail from you, run a virus scan and change the password to your e-mail account, to prevent the hacker from accessing your account again.

Bad guys are out there trying to obtain your passwords or other personal information, by a scheme called "phishing." The phishing e-mail might appear to come from a trusted "from" and "reply to" address belonging to someone you know or a business you deal with, such as your bank, a delivery company (such as UPS or Fed-Ex), or Amazon. The message might contain a link and a short message (sometimes in broken English) urging you to click on the link or open an attachment. If an attachment is a zip file or any executable file, be extremely careful! Don't open it unless you are positive it is safe. Otherwise, it might allow a bad guy to take remote control of your computer, encrypt all of your files, or make your computer as usable as a brick.

Be wary of a bank e-mailing you an urgent request to verify your account by resubmitting some account information or entering your password, Social Security number, credit-card number, birth date, or mother's maiden name. Don't do it! If your Internet Service Provider says it will suspend your account if you don't enter your password, don't do it! These are examples of phishing from fake sources. Their emails might look legitimate, with logos, etc. You can go directly to the bank's or ISP's site, without clicking on the e-mailed link, to verify your account status.

Treat all e-mails with suspicion. Do not reply to them if they ask you to confirm account information. If you need to confirm that the e-mail is legitimate, log onto the Web site of the company that supposedly sent you the e-mail. Never e-mail personal information. If the e-mail is from what appears to be a legitimate company (such as your bank) and asks you to click on a link, hover your mouse over that link and see if the address agrees with the ad-

Captain's Corner Continued from page 1

dress shown in the e-mail. If it doesn't, it's probably a scam. Watch out for the "hovered" address looking like the real thing, but it isn't. For example, a lower-case L ("l") in the legitimate address might be replaced by a one ("1") in the criminal's address, which you might not no-tice.

The scariest is ransomware, which gains access to your computer via an e-mail attachment or by clicking on something on a Web site. Even clicking on an ad on a legitimate Web site, such as a local newspaper's site, can infect your computer with ransomware (or other bad stuff). The webmaster for that site might not have been careful enough to screen a recently placed ad. If suddenly, after clicking on an ad or file, you see a little window indicating that it is screening your computer for viruses, turn off your computer immediately. That unsolicited scan might actually be depositing ransomware. You might then have to reboot your computer in safe mode (F8) and scan for viruses or ransomware. It might be too late! If ransomware locks your computer and all its files, you will probably see a notification on your monitor to pay (sometimes in bitcoins) to have the files unlocked, usually by a decryption key. If payment is not made immediately, the ransom amount might increase later. OCSD now has a Cyber Crimes Detail that might be able to help, especially in cases of ransomware infecting business or government computers.

Image files attached to an e-mail might also contain viruses or ransomware. Some e-mail clients will preview attached images automatically. Disabling the image preview pane is recommended in that case.

Don't look for trouble. Stay away from the "Dark Web." It can only be accessed by a specific browser, which is anonymous. Once you access the Dark Web, you will be pinged by bad guys and will be opening up yourself to a cyber attack.

Complex passwords will help to protect you from cyber crimes, such as hacking into your e-mail or other online accounts. Use a password of at least 12 characters (14 are better), using upper and lower case letters, numbers, and special characters. Don't use your name, your street name or address numbers, your call sign, your telephone number, or other words that could be easily guessed. Avoid dictionary words, even spelled backwards, and even with numbers tacked on. Begin the password with a symbol rather than a letter or number. To help you remember, part of your password could be the first letter of each word in a phrase (such as "maiafd" for "my antenna is a folded dipole"). Use a different password on each log-in account, and change it periodically. Software is available for storing your passwords, if you can't remember them. However, I don't recommend storing your passwords on your computer with that software, just in case a bad guy hacks into that software and discovers all of your passwords. Store your passwords on a flash drive instead (and don't leave it plugged into your computer), or, better yet, on a piece of paper.

Don't fall for someone (usually with an Indian or Pakistani accent) who calls you on your telephone, claiming to represent Microsoft and saying that your computer is infecting the Internet. The bad guy then says he can fix your computer if you give him remote access. Just hang up! Otherwise, if you give him access, he will steal information from your computer and infect it with malware, viruses, and maybe even ransomware.

In case you are cyber-attacked, I hope you have backed up your computer data. But be sure to disconnect your backup device after each backup, to prevent it from being infected during an attack. A ransomware attack will often go after all computers and backup drives on a home network, so run only one computer at a time, if possible. In fact, turn off your computer if you're not using it. Even though you might have an effective firewall to prevent intrusion, turning off your computer effectively severs an attacker's connection.

To reduce the possibility of infection, keep updating your operating system, software, and firmware on digital devices. Some of my friends advocate not performing these updates right away, to see if update bugs are reported. However, I recommend updating immediately, because the updates typically address current security issues. Set your antivirus and antimalware software to update automatically and to conduct regular scans. Back up data regularly and verify the integrity of those backups regularly, and be sure to disconnect the backup drives from your computer when not in use.

Keep your firewall turned on. It will help prevent hackers from gaining access to steal passwords, financial information, or other critical data. The latest operating systems typically have an embedded firewall, but firewall software may be purchased or downloaded if necessary. Hardware routers also typically have firewall protection.

In addition to antivirus software, running antimalware or antispyware is also recommended. If your computer is infected with spyware, bad guys may peer into your activities on the computer. Some spyware collects information about you without your knowledge or produces obnoxious pop-up ads on your Web browser. Some current operating systems offer free spyware protection, and inexpensive software may be downloaded. Be wary of some downloadable antispyware, however. It may actually contain spyware or other malicious code. One good choice for antimalware software appears to be Malwarebytes. Another choice is SUPERAntiSpyware.

Next OCRACES Meeting: May 1st

Brenda Emrick, KI6EXL, will be the guest speaker at the next OCRACES meeting on Monday, April 3, 2017, at 7:30 PM, at OCSD Communications & Technology Division, 840 N. Eckhoff Street, Suite 104, in Orange. Brenda's presentation, "Take Action: Preparedness," will be on measures that only work if we truly take action and do something! Come share an evening of friends, communications, and knowledge sharing about preparedness action steps you can take or improve upon to help make you resilient. Brenda is a Fire Protection Specialist and Community Education Officer with the City of Costa Mesa Fire Department. She has over 29 years' experience in the public education field. Brenda coordinates the citizen and business preparedness programs including: the Community Emergency Response Team (CERT); workplace, campus, and teen CERT programs; the Citizens Fire Academy; adult and youth safety programs; and CPR/First Aid training. She is the lead instructor trainer for Orange County CERT and Teen CERT programs and a national Instructor for FEMA. She currently serves as a liaison and subject-matter expert to the California State CERT Workgroup and the ReadyOC Advisory Committee in support of citizen preparedness and volunteerism.

Next City/County/MOU ACS Exercise: May 6th

The next City/County RACES & MOU ACS Exercise will be on Saturday, May 6, 2017, from 9:00 AM until 11:00 AM. The scenario for this exercise will be civil disturbance and civil disorder, also known as civil unrest. Civil disorder can include a form of protest against major socio-political problems. It is essentially the breakdown of orderly society. Examples include illegal parades, sit-ins, riots, sabotage, gang violence, shootings, car jackings, pot parties, cybercrime, immigration issues, threats of terrorism, and other forms of crime. The role of RACES would be to observe and report, and to provide backup communications to our agencies.

For the exercise, each City shall construct at least nine messages, then transmit to designated other Cities while exchanging message traffic with OCRACES and the Hospital Disaster Support Communications System (HDSCS). Messages shall be on the approved modified ICS 213 form, which may be downloaded from the "Forms" page on the OC-RACES Web site at http://www.ocraces.org/forms.html. Click on "ICS 213 Compliant Amateur Radio Message Form."

The countywide Winlink system will be exercised, with some messages to include an attachment, such as an ICS 213 form. Other messages will be sent by e-mail.

The primary modes to be used in this exercise are "General" (messages on County and City primary frequencies), "Simplex," "HF" (on 7250 kHz lower sideband), and "Winlink." We might also test DMR on the "Local 1" talk group (TG 3181, time slot 1) of the KA6P DMR repeater on Santiago Peak, on 449.0375 MHz, CC1. Some messages may be sent by Internet e-mail.

The OCRACES, City RACES, and MOU frequencies listed in the 2017 "Yellow Book" shall be used for this exercise unless changed by OCRACES or by a City or MOU Coordinator. (146.595 MHz is now the OCRACES primary 2meter simplex frequency. 147.480 MHz and 146.520 MHz have been deleted as simplex frequencies.

Emergency Communications Causes Growth

An April 11th article, "Emergency Communications Driving Increase in Amateur Radio Operators," in *Emergency Management* magazine links the growth in Amateur Radio numbers to interest in emergency communications.

"There has been a tremendous amount of interest in emergency preparedness since 9/11 and Katrina, and this is true for the Amateur Radio community as well," ARRL Emergency Preparedness Manager Mike Corey, K11U, told the publication. "Emergency communications is a gateway into amateur radio, and many join our ranks through an interest in being better prepared themselves and as a way to serve their community."

The article cites numbers from ARRL VEC Manager Maria Somma, AB1FM, who notes that 2016 was the third year in a row that the total number of new licenses exceeded 30,000.

The article also cites ARRL Colorado Section Manager Jack Ciaccia, WMØG, who agreed with the premise that the uptick in new licenses is due to amateur radio's emergency capabilities.

"Interest really peaks after a large-scale event where ham radio has been utilized," Ciaccia said. "When regular phone service fails, amateur radio operators fill the communications gap with their independent transceivers and battery power backups," said the article, which also discusses the Amateur Radio Emergency Service (ARES).

KM6CAO Hides in Lake Forest

Matt Luczko, KM6CAO, was the fox on Monday, April 17, 2017, on the monthly cooperative T-hunt. He turned on the fox box immediately following the 2-meter OCRACES ACS net, hiding in Lake Forest behind the Orange County Library near El Toro Road and Raymond Way.

First to find the fox, in less than 10 minutes, was Richard Saunders, K6RBS. Next was Ken Bourne, W6HK. Riding with Ken and manning the loop was Brian Ahn, KM6CXL. They started at El Toro Road and Trabuco Road, and were befuddled by bad bearings, probably caused by buildings blocking and reflecting the signal. Furthermore, Randy Benicky, N6PRL, who was with the fox, repositioned the fox-box antenna to a horizontal position after the hunt started, causing inaccurate bearings on the hunters' vertical beam and loop.

The next cooperative T-hunt will be held on Monday, May 15, 2017, immediately following the OCRACES 2-meter net

(approximately 7:20 PM). The fox will transmit on the input (146.295 MHz) of the 146.895 MHz repeater. Hunters will compare bearings via the 448.320 MHz repeater (while the 449.100 MHz repeater is down), and are encouraged to beacon their positions via APRS throughout the hunt. The fox will be hiding in a city or sector of Orange County (to be announced a few days prior to the hunt) on paved, publicly accessible property. No fees will be required to drive directly to the fox. We are looking for a volunteer to be the fox, and a "fox box" will be available.

The cooperative T-hunts are usually held on the third Monday of each month. The hunts provide excellent practice in working together to find sources of interference quickly. The hunts are not official RACES events, so DSW (Disaster Service Worker) coverage does not apply. Please drive carefully!

Fox-hunt loops and beams are available from Arrow Antenna and HRO, including the Arrow Model FHL-VHF foxhunt loop (covers 1 MHz to 600 MHz) and the Arrow Model 146-3 three-element portable hand-held yagi. The Arrow OFHA 4-MHz offset attenuator can be useful when close to the fox, to prevent receiver overload. An all-mode transceiver is quite useful, allowing hunters to switch to the SSB or CW mode for detecting extremely weak signals, or to switch in a built-in attenuator, reduce RF gain, or tune slightly off frequency when dealing with extremely strong signals. Some hunters use the DF2020T radio direction finder kit, which is a Doppler system available from Global TSCM Group, Inc. (http://www.kn2c.us). A very similar system is the MFJ-5005 Doppler direction finder. Other useful tools are the Foxhunt app for iPhones and the Triangulate app for Android phones.

Grounding and Bonding for the Radio Amateur

Grounding and Bonding for the Radio Amateur by Ward Silver, NØAX, is now available from ARRL. Proper station grounding is important! Build your ham radio station with effective grounding and bonding techniques:

- AC safety: protects against shock hazards from AC-powered equipment by providing a safe path for current when a fault in wiring or insulation occurs.
- Lightning protection: keeps all equipment at the same voltage during transients from lightning and dissipates the lightning charge in the earth, routing it away from equipment.
- RF management: prevents unwanted RF currents and voltages from disrupting the normal functions of equipment (also known as RF interference or RFI).

Grounding and Bonding for the Radio Amateur shows you how to make sure your station follows current standards for lightning protection and communication systems, not to mention the National Electrical Code. You'll learn effective grounding and bonding techniques for stations in a house, condo, or apartment, for portable and temporary situations, and for towers and outdoor antennas.

Grounding and Bonding for the Radio Amateur is available from the ARRL Store or your ARRL Dealer. (ARRL Item no. 0659), ISBN: 978-62595-0659, \$25.95 retail, special ARRL Member Price \$22.95). Call 860-594-0355 or, toll-free in the US, 888-277-5289. It is also available as an e-book for the Amazon Kindle.



At the fox's den are (left to right) Randy Benicky, N6PRL, Brian Ahn, KM6CXL, Matt Luczko, KM6CAO (the fox), and Richard Saunders, K6RBI.

EOC Offers Training Opportunities

The Orange County Emergency Operations Center is offering some training opportunities to all County employees and Operational Area Partners, as well as OCRACES members, over the next two months. See the course descriptions below: **May**

Мау

• EOC Response: Action Planning, Information Analysis, Situation Awareness, May 11, 8:00 AM to 12:00 PM This course is designed for agencies and jurisdictions who may fill a Planning and Intelligence Section position within the EOC to maintain information management and situational analysis. Training will include an overview of the Planning and Intelligence Section, consequences management, EOC Action Planning process, and training on specific emergency plans and annexes maintained by the Emergency Management Division. Training will include hands-on practice and training on position-specific roles and responsibilities.

• Web EOC 8.0/JIMS 8.0, May 17, 9:00 AM to 11:00 AM This is a 2-hour class on the WebEOC Incident Management System used in Emergency Operations Centers. The WebEOC system has been completely redesigned and this course will demonstrate how to use the new WebEOC and JIMS 8.0 version. The class is a hands-on tutorial including log-in procedures, Activity Logs, and the Jurisdictional Information Management System. Enrollment is open to all County employees and Operational Area Partners.

June

- EOC Response: *Logistics & Finance Section*, June 8, 9:00 AM to 11 AM This course is designed for those who may fill a Logistics & Finance Section position within the EOC. Training will include an overview of the Logistics & Finance Section process, protocols, position checklists, and hands-on practice. Enrollment is open to all County employees and Operational Area Partners.
- Web EOC 8.0/JIMS 8.0, June 14, 9:00 AM to 11:00 AM
- Intro to SIMS, NIMS, ICS, and EOC Orientation, June 20, 1:00 PM to 3:00 PM This introductory course is intended to give participants a basic overview of the Incident Command System, Standardized Emergency Management System, National Incident Management System, and an orientation to the basic functions of the County Emergency Operations Center.

To register, please download the registration form from the "Forms" page on the OCRACES Web site at http:// www.ocraces.org/forms.html. Click on "EOC Training Registration Form January to June 2017." Then e-mail Miriam Aldana at maldana@ocsd.org.

OCRACES to Team with OCARC on Field Day

It was decided at the April 3rd OCRACES meeting that we will team up with the Orange County Amateur Radio Club (OCARC) for Field Day on June 24-25, 2017, like we did last year. We appreciate Brad Russo's ambitious proposal for our own Field Day, but there is not enough time to put together such an extensive operation between now an June 24-25. Maybe we can go in that direction next year. Field Day is still a required event for all OCRACES members. We will learn from the OCARC members who are highly experienced in successful Field Day operation, and they will learn from us, as we work together for a highly successful event. Planned modes for this year include 40 meters CW, 40 meters phone, 20 meters digital, 20 meters CW, 20 meters phone, VHF/UHF phone, satellite, and GOTA (10/15/80 meters).

Field Day will be at the Walter Knott Education Center at 7300 La Palma Avenue in Buena Park. Setup will be on Friday morning, June 23rd, and Saturday morning. Operations will be from Saturday at 11:00 AM until Sunday at 11:00 AM. Teardown and group photo will be from Sunday at 11:01 AM until done.

Peace Officers' Memorial Ceremony: May 25th

The Orange County Chiefs' of Police and Sheriff's Association and the Orange County Sheriff's Advisory Council invite you to attend the 2017 Orange County Peace Officers' Memorial Ceremony at 7:00 PM on Thursday, May 25, 2017, at the Orange County Peace Officers' Memorial Monument, Orange County Sheriff's Regional Training Academy, 15991 Armstrong Avenue, in Tustin. A Candlelight Vigil immediately follows, and both ceremonies are combined into one event to remember the officers who have made the ultimate sacrifice "In The Line Of Duty."

RACES/MOU News from Around the County

"RACES/MOU News" provides an opportunity to share information from all City & County RACES/ACS units and MOU organizations in Orange County.

Please send your news to NetControl Editor Ken Bourne, W6HK, at:

w6hk@ ocraces.org

<u>Hospital Disaster Support</u> <u>Communications System (HDSCS)</u>

HDSCS hosted the first of three amateur radio licensing exam sessions for 2017 on Saturday, April 8, 2017, at Care Ambulance in Orange. At the session, one of the Orange County EMS staff passed the Technician test. Another test session will be held at the HDSCS 2017 Field Day and the third session will be in October. Information will be on the ARRL Web site.

HDSCS participated in the Orange County Multi-Agency Disaster group spring drill on Wednesday, April 12, 2017. The morning drill scenario involved a large earthquake shaking the County, causing power outages, loss of communications, and freeway damage. HDSCS members activated in accordance with their automatic response plan. The communicators checked in with the net control, indicating their location and what hospital or hospitals they were closest to. The net control would then advise operators as to where the greatest need was at the time. Typically trauma centers and paramedic base stations have priority. As HDSCS has in some real earthquake responses, some communicators checked on and communicated from more than one hospital in the drill. Members were challenged with some evacuation issues, relocation of command centers, and getting resource requests to County EMS. It wasn't an easy exercise but comments from the EMS Medical Director made it worth the effort. "HDSCS was praised over and over for their participation and help in the Wednesday drill. The hospitals were very happy to have HDSCS support, and in the EMS Departmental Operations Center it was very helpful."

This year's HDSCS Orientation and Review Workshop will be on Saturday, April 22nd. The all-day workshop will cover such topics as the hospital environment, the value of the ARES structure for supporting hospitals, basic radio operations in the hospital, Hospital Incident Command System, and handling messages relative to patient care. Attendees will also participate in the traditional "Disaster Potluck" during the noon hour. A limited number of communicators from other emergency groups may attend. Those interested should contact April Moell, WA6OPS, at emcom4hosp@aol.com

Orange County SKYWARN

The National Weather Service in San Diego has advised weather spotters that, when you log onto weather.gov/SanDiego (which redirects you to http:// www.weather.gov/sgx/), you will find a new Web page. The content is there but the look and feel is quite different. There are also links to national products and also icons for quick links.

The "Submit Report" link is under the "Current Hazards" tab (which is to the left, just above "Today's Highs."

NWS San Diego says, "Remember when submitting reports be sure to go through each step completely and 'acknowledge' the preview of the report by clicking the small check box, otherwise the report will not be transmitted to us."

Cal OES CRU

Bill Pennington, WA6SLA, Chief State ACS/RACES Officer, has announced that the Cal OES ACS organization is now called the Communications Reserve Unit (CRU). Although still functional under the Auxiliary Communications Service (ACS) Program, this better identifies what the unit does with regard to emergency communications statewide. The CRU staff provides public-safety communications for many county, state, and federal agencies within the state. CRU provides public-safety communications by deploying radio, telephone, and data equipment for both state and federal fires, search-and-rescue incidents, flooding, and other incidents as required. At the same time, the amateur radio portion of the CRU will still be active under the ACS Program with statewide California Emergency Services Nets and region VHF and UHF nets.

May 2017

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1 Weekly 2 m ACS Net & OCRACES Meeting	2	3	4	5	6 City/County RACES & MOU ACS Exercise
7	8 Weekly 2 m ACS Net	9	10	11	12	13 Weekly 40 m ACS Net
14	15 Weekly 2 m ACS Net & Cooperative T-Hunt	16	17	18	19 OCARC Meeting	20 Weekly 40 m ACS Net
21	22 ACS Nets on Five Bands & Cal OES Nets	23	24	25 OC Peace Officers' Memorial Ceremonies	26	27 Weekly 40 m ACS Net
28	29 Memorial Day (no net)	30	31			

Upcoming Events:

- May 1: OCRACES Meeting, 840 N. Eckhoff Street, Suite 104, Orange; 1930 hours
- May 6: City/County RACES & MOU ACS Exercise, 0900-1100 hours
- May 15: Cooperative T-Hunt on input of 2-meter repeater, 1920 hours
- May 19: Orange County Amateur Radio Club Meeting, American Red Cross (George M. Chitty Building), 600 Parkcenter Drive, Santa Ana; 1900 hours
- May 22: ACS Nets on five bands and Cal OES Nets from OC EOC
- May 25: Orange County Peace Officers' Memorial Ceremonies, Orange County Peace Officers' Memorial Monument, Orange County Sheriff's Regional Training Academy, 15991 Armstrong Avenue, Tustin; 1900 hours
- May 29: Memorial Day (no net)
- June 24-25: Field Day with the Orange County Amateur Radio Club





Mission Statement

County of Orange RACES has made a commitment to provide all Public Safety

departments in Orange County with the most efficient response possible to supplement emergency/disaster and routine Public Safety communications events and activities. We will provide the highest level of service using Amateur and Public Safety radio resources coupled with technology, teamwork, safety, and excellence. We will do so in an efficient, professional, and courteous manner, accepting accountability for all actions. We dedicate ourselves to working in partnership with the Public Safety community to professionally excel in the ability to provide emergency communications resources and services.

County of Orange RACES Frequencies

40 m: 7250 kHz SSB (City/County/MOU Net—Saturdays, 1000 hours) 10 m: 29.640 MHz output, 29.540 MHz input, 107.2 Hz PL 6 m: 52.620 MHz output, 52.120 MHz input, 103.5 Hz PL 2 m: 146.895 MHz output, 146.295 MHz input, 136.5 Hz PL* 2 m: 146.595 MHz simplex 1.25 m: 223.760 MHz output, 222.160 MHz input, 110.9 Hz PL 70 cm: 446.000 MHz simplex 70 cm: 448.320 MHz output, 443.320 MHz input, 141.3 Hz PL (private) 70 cm: 449.100 MHz output, 444.100 MHz input, 110.9 Hz PL (out of service) 70 cm: 449.180 MHz output, 444.180 MHz input, 107.2 Hz PL (private) 23 cm: 1287.650 MHz, 1287.675 MHz, 1287.700 MHz, 1287.725 MHz, 1287.750 MHz, and 1287.775 MHz outputs, -12 MHz inputs, 88.5 Hz PL

*Primary Net—Mondays, 1900 hours

RACES Program Coordinator (Emergency Comm's Manager) Lee Kaser, KK6VIV 714-704-8080

Radio Officer (Lieutenant) Scott Byington, KC6MMF <u>Chief Radio Officer (Captain)</u> Ken Bourne, W6HK 714-997-0073

Assistant Radio Officers (Sergeants) Jack Barth, AB6VC Ernest Fierheller, KG6LXT Bob McFadden, KK6CUS Tom Tracey, KC6FIC

County of Orange RACES

OCSD/Communications & Technology 840 N. Eckhoff St., Suite 104, Orange, CA 92868-1021 Telephone: 714-704-8080 • Fax: 714-704-7902 E-mail: ocraces@comm.ocgov.com

County of Orange RACES

OCSD/Communications & Technology 840 N. Eckhoff St., Suite 104, Orange, CA 92868-1021

Telephone - 714-704-8080 Fax - 714-704-7902 E-mail - ocraces@comm.ocgov.com



Questions or Comments? Contact NetControl Editor Ken Bourne, W6HK w6hk@ocraces.org



"W6ACS Serving **Orange County**"

Meet Your County of Orange RACES Members!

AB6VC



Ken Bourne W6HK

Scott Byington KC6MMF



KM6BV



Ernest Fierheller KG6LXT



Tom Tracey KC6FIC



Randy Benicky N6PRL

Roger Berchtold WB6HMW



Jim Dorris KC6RFC

Nancee Graff N6ZRB



Ray Grimes N8RG

KK6CUS



Walter Kroy KC6HAM



Martin La Rocque N6NTH



KM6CAO

FRAN

Fran Needham KJ6UJS



Kenan Reilly KR6J



Tom Riley Brad Russo K6TPR KB6GPM





Joe Selikov KB6EID

Robert Stoffel KD6DAQ

Ken Tucker WF6F



KJ6SPE

Bob McFadden





Lee Kaser KK6VIV



