

THE CPIRC NEWS

VOLUME IV, ISSUE II MAY 2004

CCTV BLOW-OUT SALE

Between May 24th and June 24th the CPIRC Surveillance Shop will drop prices on all pinhole cameras, bullet cams, covert cameras, DVR's, time lapse recorders, wireless transmitters and receivers, and much, much, more. Check out some of these prices:

- CCD B/W Pinhole Camera **\$65** (taxes included)
- Covert PIR Camera **\$149** (taxes included)
- Wireless Transmitter & Receiver Kit **\$249** (taxes included)
- 4 Channel Digital Video Recorder **\$1299** (taxes included)
- Mobile Time Lapse Recorder **\$499** (taxes included)

Visit the Surveillance Shop at www.cpirc.com.

All prices are in Canadian dollars. All items come with a 1 year warranty.



INSIDE THIS ISSUE

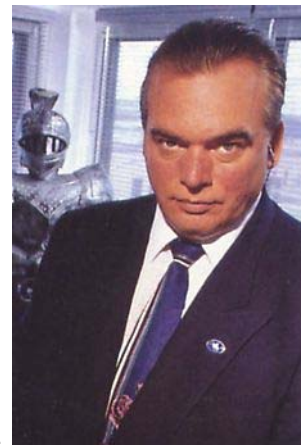
CCTV BLOW-OUT SALE	1
IN MEMORY OF CRAIG H. BEST (1954-2004)	2
THE RESOURCE CENTRE ROUND-UP	3, 10-11
PROPOSED CHANGES TO THE P.I. FIELD IN QUEBEC	4-5
THE USE OF SPIES	6
YEAH, SO WHO ASKED YA?	7-9
CONTACT INFORMATION	12

IN MEMORY OF

Craig H. Best (1954-2004)

We would like to dedicate this issue to a man who has devoted his life to the security and law enforcement field. Craig H. Best passed away on Tuesday May 11, 2004 at the age of fifty, after a long and courageous battle at the Montreal Jewish General Hospital.

Craig's career included 30 years of experience as a police officer, personal protection agent and private investigator. He was an instructor trainer in Firearms, PR-24, M.E.B., Scepter Baton, Officer Survival, Executive Protection, Police Pressure Point System, O.C. Aerosol (pepper spray) and so much more. He was also a court expert witness in the subject of "Use of Force". He was a leader, trainer and mentor to thousands of police and security professionals whose lives he touched internationally. Craig was involved with Monadnock since its early days and was the first and only Canadian International Instructor only to be replaced by Jocelyn Moisan and Robert C. White of the Pro-vision Group International who he personally hand picked before his passing. Everyone at the Canadian Private Investigators' Resource Centre would like to congratulate you both and we're sure that you will make Craig proud.



A memorial service will be held at the Côte Des Neiges funeral center (4525 Ch. De la Côte Des Neiges, Montreal. Tel: 514-342-8000 or 1-800-342-6565) on Monday May 24th, 2004 from 14:00 to 17:00 and 19:00 to 22:00. The service which will be followed by the burial will be held on May 25th, 2004 at 10:00 am.

If anyone would like to send a message to Craig's family you may email us at info@cpirc.com and we will forward all messages to Craig's family.

RESOURCE CENTRE ROUNDUP

With **eComp Online** you may search:

- Compensation data on 50,000 Senior Executives.
- Review Board of Directors' Pay Practices at 1,500 U.S. Companies.
- Create peer groups and benchmark against industry standards.
- Analyze Cash & Equity Comp. and compare against company performance.
- Instant access to recent equity awards as reported in Form 4 filings.

A quick search on Nortel Networks came up with the following results:

- F.A. Dunn, President and CEO, received \$825,000 in 2002. But sadly, he received no bonus for that year.

Click on the **eComp Online** link found in the **“Business/Land Titles/Personal Property”** category in the Resource Centre.

What's CarProof?

CarProof has electronic access to the jurisdictional government databases across Canada to bring car dealers and consumers current critical data on vehicles that are, or were ever, registered in Canada. The results of your search request are delivered to you by email in a printable document format.

What do you get in a CarProof report?

Using your Vehicle Identification Number, they check the databases of each Ministry of Transportation in Canada, including the Territories and report back with the following vehicle history: 1. Stolen 2. Salvage 3. Rebuilt 4. Non-Repairable 4. Unfit 5. Abandoned 6. Moved 7. Liens.

Click on the **CarProof Vehicle History** link found in the **“Planes, Trains and Automobile Related Sites”** category in the Resource Centre.

Improving your memory is one of many essential skills that every investigator should always be working on.

Click on the **Improve Your Memory** link found in the **“Virtual Reference Desk”** category in the Resource Centre.

We have added several links to live cameras across Canada such as:

- Ontario Traffic cams
- Regina Airport
- St. John's Harbour
- Tourist sites & traffic cams in Montreal.
- Several Canada/U.S. border cameras.

Click on the **Live Web Cams & Road Conditions** link found in the **“Planes, Trains and Automobile Related Sites”** category in the Resource Centre.

History is filled with great people involved in the espionage business. Did you know that Galileo sold spy gear?

In 1608 Galileo was introduced to a new toy from the Netherlands. When he would peer through this rigid tube with a glass lens at both ends it made objects that were several feet away appear closer. After months of fiddling with the toy he found a way to dramatically increase the magnification of what he saw by 20 times. He soon sold his spyglass to an eager Venetian navy that would use it to spot enemy ships hours before they entered the Venetian harbour. We now know the spyglass as a telescope.



Galileo Galilei
(1564 - 1642)

Louis Laframboise, COO of Chartrand Laframboise sent us his thoughts on the proposed changes to the Security/Investigation field in Quebec and we thought many of you may find it interesting. You may download a copy of the Quebec government's proposed changes from our Resource Centre in the "**Courts/Lawyers/Law Advice/ PIPED Act**" category.

We would also like to congratulate Louis Laframboise in receiving the 2003 Investigator of the Year Award during World Association of Detective's (W.A.D.) 78th Annual Conference held in Honolulu, Hawaii on October 4th, 2003.

This Investigator of the Year Cup is awarded to a W.A.D. member who has performed outstanding investigations in the best traditions of the profession.

Louis Laframboise is a Past President of the World Association of Detectives and is a Director of Investigations Canada.

SUMMARY OF THE EFFECTS OF THE WHITE PAPER ON PRIVATE SECURITY AND INVESTIGATION

The Quebec government has recently released a White Paper entitled Private Security: Partner in Internal Security proposing compliance requirements that would add bureaucracy to investigations by the private sector, such as a mandatory registration system and public sector oversight. Criminal investigations will be particularly affected. Using "Operation Spring Fever" of a few years ago, as an example, where some life and health insurers became the victim of systemic fraudulent activities in the Montreal area, a formal protocol with the Ministry concerned would have to be signed and its terms and conditions would have to be followed.

According to the Conseil du patronat du Québec (a provincial association of employers), the White Paper proposals, if adopted, will have major implications on all private enterprises operating in the province. A centralized and intrusive approach to investigations will basically constitute the new regime.

The Quebec government's proposals to reform the outdated regulatory framework governing investigations and security in the private sector, were discussed on February 5, 2004 in Montreal at a very large gathering of the parties concerned. The proposed new framework is outlined in a 83-page White Paper that was issued by the Quebec Public Security Minister on December 16, 2003. Public hearings before a parliamentary commission began (Feb 10th) and will continue later in the Spring. The Minister indicated that there is no urgency to legislate rapidly.

The reform was found to be far reaching, too prescriptive, intrusive of business management, lacking compliance cost evaluations, vague on several key points, too critical of current practices, and inaccurate in terms of realities.

The following proposals are of particular interest as an example to life and health insurance companies, but also to all companies that may have in house investigators or that will require contractual resources:

- √ In-house investigations and security functions of all kinds would be caught by the new framework.
- √ Insurers doing investigations would be required to hold an investigative agency license.
- √ Employees doing investigations would have to be individually licensed as investigative agents.

√ Because different activities would be subject to separate licensing, multiple licenses would be necessary. For example, surveillance, the collection and analysis of personal information, and the detection of computer crimes would require three distinct licenses.

√ Specific education, training, ethics and supervision requirements would be mandated for each license.

√ Membership into an association of peers would most likely be mandatory (for disciplinary measures).

√ All investigations of a criminal nature from stealing company pencils to making fraudulent insurance claims would have to be reported to the police.

√ No "privilege" status would be granted to reporting entities (none is proposed in the White Paper).

√ Certain activities would have to comply with government approved service agreements.

√ Outsourced investigations and security tasks would equally fall under the new regime.

√ All costs associated with the regulatory provisions (once provincial legislation is enacted) would be borne entirely by Quebec's investigation and security industry and its players.

Louis Laframboise, C.F.E. is the Chairman & C.O.O. of Chartrand Laframboise, a private investigation and security firm in business since 1986. He is the current Chairman of the World Associations of Detectives inc., a member of ASIS International's Investigation's Council and President of the Montreal Chapter of the Association of Certified Fraud Examiner, a proud partner of Investigations Canada and has been a member of the Canadian Private Investigators' Resource Centre since 2000. Louis has experience in law enforcement with the R.C.M.P., as corporate security with the Royal Bank of Canada and as a private investigator with a multitude of clients, at the local, national and international levels. His work experiences and his constant participation in conferences world wide, in the field of private investigation and security, keep him abreast of the trends.

Louis Laframboise can be reached through the www.chartrand-laframboise.com website or via email at gen@chartrand-laframboise.com.

Sun Tzu's **THE ART OF WAR**

Chapter 13: **THE USE OF SPIES**

Sun Tzu said: Raising a host of a hundred thousand men and engaging them in war entails heavy loss on the people and a drain on the resources. The daily expenditure will amount to a thousand ounces of silver. There will be commotion at home and abroad, and men will drop out exhausted.

Opposing forces may face each other for years, striving for the victory which may be decided in a single day. This being so, to remain in ignorance of the enemy's condition simply because one grudges the outlay of a hundred ounces of silver is the height of stupidity.

One who acts thus is no leader of men, no present help to his cause, no master of victory. Thus, what enables the wise commander to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge. Now this foreknowledge cannot be elicited from spirits; it cannot be obtained inductively from experience, nor by any deductive calculation. Knowledge of the enemy's dispositions can only be obtained from other men.

Hence the use of spies, of whom there are five classes: **1. Local Spies** - Having local spies means employing the services of the inhabitants of an enemy territory; **2. Moles** - Having moles means making use of officials of the enemy; **3. Double Agents** - Having double agents means getting hold of the enemy's spies and using them for our own purposes; **4. Doomed Spies** - Having doomed spies means doing certain things openly for purposes of deception, and allowing our spies to know of them and report them to the enemy; **5. Surviving Spies** - Surviving spies means are those who bring back news from the enemy's camp.

When these five kinds of spy are all at work, none can discover the secret system. This is called "divine manipulation of the threads." It is the commander's most precious faculty. Hence it is that which none in the whole army are more intimate relations to be maintained than with spies. None should be more liberally rewarded. In no other fields should greater secrecy be preserved.

1. Spies cannot be usefully employed without a certain intuitive sagacity; 2. They cannot be properly managed without benevolence and straight forwardness; 3. Without subtle ingenuity of mind, one cannot make certain of the truth of their reports; 4. Be subtle! be subtle! and use your spies for every kind of warfare; 5. If a secret piece of news is divulged by a spy before the time is ripe, he must be put to death together with the man to whom the secret was told.

For more on The Use of Spies pickup **The Art of War** by Sun Tzu at your local bookstore.



Sun Tzu, Chinese general, circa 500 B.C. A collection of essays on the art of war is attributed to Sun Tzu. There are a growing number of translations of this Chinese classic, usually titled *The Art of War*.

Knowledge of Sun Tzu reached Europe shortly before the French Revolution in the form of a summary translation by Father J. J. M. Amiot, a French Jesuit priest. In the various translations, Sun Tzu is sometimes referred to as Sun Wu, and Sun Tzi. The most fundamental of Sun Tzu's principles for the conduct of war is that "All warfare is based on deception". Another key Sun Tzu principle is that "The supreme art of war is to subdue the enemy without fighting." Sun Tzu's ideas spread to the rest of Asia and to Japan.

Yeah, So Who Asked Ya?

By John A. Nolan, III CPP, OCP

Over the course of the past few years, readers have asked about the things that our experience in collecting information from employees tells us. Lessons learned about how much employees talk and say far more than they should when we contact them. Lessons that we have learned that security managers can use in their in-house briefings about protecting sensitive or proprietary information.

Usually, I respond to those readers individually, but frankly, the questions are getting to be so frequently asked that I'm almost tempted to copy and forward previous responses. But, rather than doing that, I think it might be better to just approach it in one article for Security Technology and Design.

So, we're going to talk a little about how we do Competitive Intelligence work, as a background, for the lessons that we've learned over the years. And frankly, we're not really worried too much that by telling you gentle readers how we do things and what they mean, that we'll wind up unable to talk to your employees and thus, not be able to do our jobs for our clients. I don't say that out of boasting or anything like it.

The reason that I don't hesitate to talk a little about our way of doing things is that a considerable number of you won't believe what I'm about to say. Others will believe it, but haven't developed any way of disseminating the information to their employees. And yet still others, even if they do take it to heart, the greatest majority won't do much more with the information than put it into a file and it'll sit there, unread by and unknown by their employees.

And you're sitting there saying to yourself, "What a jerk this guy Nolan is! Saying these things to me. Who does he think he is? As if he thinks he can get away with getting in my face, challenging me to improve the way we do our business! I'm a security professional. I don't need his grief." If you'll hold on a second, I'll explain.

As you read at the outset, lots of people have e-mailed me or called me about countering threats to their proprietary and sensitive information. I've told them repeatedly what I'm going to tell you here.

We've sent information about protecting companies from people who operate in the Competitive Intelligence business to many security managers who read ST&D. As business turns, we've been asked to conduct intelligence collection assignments against an even dozen of those companies where the security managers had previously asked us about steps to defeat our efforts. In every one of those cases, we've accepted the assignment, because that's what we do -- but with the caveat to the client that we are uncertain about our level of success because we know that the company under consideration has a security leader who is apparently involved in information protection.

But now, we don't bother with that caveat anymore. Why? Because when we try to penetrate the designated target company, we don't find it any more difficult to conduct collection operations there than in any other companies. There's no way that I can say why this is, but I've got a couple of guesses. First, the security manager just isn't really interested. Or, second, the manager took the information but didn't do anything with it. Or third, she took it and tried to disseminate it to the work force without much effect. Or last, we're just a heckuva lot better than we think we are. I tend to one of the first three possible explanations.

Competitive Intelligence 101

We don't break into buildings, challenge gates or guards or guns or dogs. We don't hack into computer systems. We don't bribe people or do anything surreptitious. We don't do midnight skulking or lurking.

We don't do Waste Archaeology, the nice way of saying dumpster diving. We don't even do ruse interviews, such as telling someone that we're graduate students working on a research project. Instead, we call people on the telephone, meet them at industry conferences, scientific symposia, technical meetings and trade shows. Because we follow the Code of Ethics of the Society of Competitive Intelligence Professionals, we always identify ourselves by our true name and company affiliation before we start any interview.

You'd think that that would keep people from talking to us, or at least to ask some questions that would cause them to be more reserved or suspicious or both. You'd be correct, too. But only to a limited degree. It's part of our business to look at trends that affect the way we do things and to change them accordingly. So, we track how people respond to our overtures. What I'm about to tell you derives from our examination of thousands of interviews over the past ten years, and the results have remained consistent during that time.

Out of every one hundred people we speak with, fifty of them will respond favourably and positively to our opening statement. For example, if I were to be calling a potential source in New York, I'll say "Hi, Fred. My name is John Nolan and I'm calling from Phoenix Consulting Group in Huntsville, Alabama. I'm working on a project and I was told that you're the smartest man who ever wore hair concerning XY and Z. Is this a good time to talk?" Fifty of these Fred's will say something like, "Yeah, this is as good a time as any. What can I do for you?"

The other fifty Freds are a little less willing. These second category people respond with something on the order of "What's Phoenix Consulting Group and what's this about?" Do we reply with some sort of fictional explanation? No. There's no need to do that. We respond that we're a research firm and that we're engaged in a project on behalf of a client. Inevitably, our respondent asks another question at this point, such as "Well, who is your client?"

Our researchers are trained to answer that we have confidentiality agreements in place with all of our clients, which extends even to the identity of the client. You'd think that at this point in such a conversation, anybody with above a room temperature IQ would say "Hey, if you're not going to tell me who your client is, this conversation is over." Click. And you'd be right. Except that this only happens to about fifteen of those remaining fifty people. The other thirty five say things like, "Oh yeah. We've gotta put up with all that confidentiality nonsense at our place too. What can I do for you?"

Think about this for a nanosecond. This means that 85% of your fellow Americans, 85% of your employees, agree to cooperate in the discussion and reveal information that is valuable to you and your firm. When we get slammed by one of those fifteen others, we take comfort in the fact that there are still a whole bunch of sources out there just waiting to talk to us -- without knowing or really caring who we are or for whom we're working.

Elicitation Techniques 101

Then, once we get the person agreeing to speak with us, we begin to abandon our direct questioning approach and turn to the intelligence officer's stock-in-trade: elicitation. Getting the information we need without asking for it. Techniques that we train Federal intelligence officers and undercover officers in several times a year. Techniques that we train Competitive Intelligence professionals in dozens of times a year -- although of course there are some techniques that we teach the Feds that we don't teach business people.

Techniques that range from a seemingly common exchange of information, certain kinds of provocative statements, disbelief, feigned naiveté, criticism, encouraging members of our society of snivellers and whiners to cry on our shoulders, and many more. Techniques that recognize a variety of human factors: a desire for recognition; tendencies towards one-upmanship (or one-downmanship, as in "Yeah, well let me tell you how bad my place is compared to yours); natural tendencies to correct others when somebody makes a mistake -- on purpose -- in the interest of getting a knowledgeable person to provide the real, and accurate, information; and ten or fifteen others..

Factors and techniques that are used in a rigorous and organized process of obtaining information in a systematic and highly effective way. Knowing which ones to use with which source, or trying out others, discarding the ones that work and noting for future use on the source card, those techniques that worked well with each individual. Knowing when to end the conversation before the target becomes concerned with the course of the conversation.

Knowing that corresponding, confirming and additional information will be forthcoming from one of the many other sources that you'll be calling during the project. Knowing that it will all add up at some point to the information you. Knowing that it's extremely rare -- and sometimes less than desirable -- to get everything you need from one individual source.

Countermeasures 101

As you can tell from the sub-course numbering, we're still at the most fundamental level. The level where it's up to you to do some thinking. Just understand that the foundation for any countermeasure is awareness of what the issue is in the first place. Perhaps this simple little discussion will cause you to think a bit about how well prepared your employees are to deal with calls or contacts from outside such as those I've described. Perhaps this will stimulate you to ask about specific kinds of countermeasures that are useful for a security manager to provide the employee population in an additional effort to safeguard your proprietary information.

If you're thinking along those lines, you've actually got a couple of options. You can wait for a future column to speak about some of the more common and effective countermeasures that we teach to people who are serious about protecting their proprietary or sensitive information. Or, you can send me an e-mail if you'd like a handful of useful and practical approaches that you may find useful in training up your employees to keep things to themselves.

Or, you can file this article away with everything else, do nothing, and embark on the exciting career of a librarian.

About the author: John A. Nolan, III CPP, OCP is Chairman and Managing Director of Phoenix Consulting Group, which provides competitive intelligence, counterintelligence and professional development/training programs across a variety of industries. He is also a co-founder of The Centre for Operational Business Intelligence in Sarasota, FL where corporate intelligence practitioners from around the country and the world learn the tools and techniques necessary to prevail in the marketplace. His newest book, **CONFIDENTIAL: Uncover Your Competitor's Top Secrets Legally and Quickly - And Protect Your Own** was released by HarperCollins Business Books in June 1999. He is frequently featured in national and international media such as Forbes, George, Times of London and CNN, to name just a few. He can be reached at <jnolan@intellpros.com>, or at 1.800.440.1724

RESOURCE CENTRE ROUNDUP (CONTINUED)

Need an Investigative Journalist?

On the Investigative Reporters and Editors Inc. website there is a list of 20 Canadian Investigative reporters. Click on the [Canadian Investigative Journalist](#) link found in the “[Newspapers/Media Contacts/Journalism Research](#)” category in the Resource Centre.

The Center for Investigative Reporting is an independent news organization that strengthens democracy by exposing

injustice and abuse of power. To achieve this, CIR:

1. **Investigates** critical, underreported issues. 2. **Produces** compelling, in-depth stories for print, broadcast and Internet news outlets. 3. **Provides** its reporting to citizens and decision makers so they can take informed action.

Click on [The Center for Investigative Reporting](#) link found in the “[Newspapers/Media Contacts/Journalism Research](#)” category in the Resource Centre.

The Nevada Gaming Commission and State Gaming Control Board has an online Excluded Person List. List includes mug shots, a physical description, aliases and description of past conviction. To access the [Nevada Gaming Commission and State Gaming Control Board](#) website click on the link found in the “[Resource USA](#)” Category in the Resource Centre.



Which Ontario cemetery is John Doe buried in?

The Ontario Cemetery Finding Aid is a pointer database consisting of the surnames, cemetery name and location of over 2 Million interments from several thousand cemeteries, cairns, memorials, and cenotaphs in Ontario Canada.

Click on the [Ontario Cemetery Finding Aid](#) link found in the “[Genealogy Research/Birth & Death Records/Adoptee Registry/Canadian Government Archives](#)” category in the Resource Centre.

The [British Columbia Securities Commission](#) website has a database where one can search reports on insider trading, cease trade information, view public filings information for Foreign Issuers and Notice of Intention to Distribute Securities.

Click on the [British Columbia Securities Commission Database](#) link found in the “[Business/Land Titles/Personal Property](#)” category in the Resource Centre.

In the bible there are approximately 132 references to espionage. The bible's first intelligence operation happened in the book of Genesis, when the Devil was able to recruit Eve as an asset to full-fill the Devil's evil plot.

Moses and Joshua also used spies to gather intelligence on their enemies. In chapter 2 of the book of Joshua, Joshua sends two spies into the land of Canaan and tells them, "Go check the land and come back with a report." The spies run right back after meeting Rehab, their informant. Of the two, Joshua was probably a better Spymaster. Unlike Moses, Joshua would listen to all information gathered from his agents in private, later making his decision on what do with the information collected. The fact is not all information collected is necessarily the truth. Part of counter-intelligence is spreading disinformation to confuse your enemy. By listening to his agents' accounts in private Joshua had the option to decide what information he would trust and what he would disregard.

INFORMATION FOR TRAVELLERS

If you're frequently traveling abroad visit our "**International & Miscellaneous**" category. You will find valuable information like:

- Travel Warnings.
- Information & Assistance to Canadians abroad.
- Find Western Trained doctors when abroad.
- Where to get your international drivers permit.
- Immunization Recommendations for International Travel.
- Find health centres here in Canada to get vaccinations.
- CIA World Factbook which contains a vast amount of information on countries around the world. It is also free to download.

JOINING NEWSGROUPS

Joining Newsgroups is a great way to stay up-to-date, share ideas, ask questions and network with others in your field without ever having to leave the comfort of your home or office. There are many Newsgroups out there relating to Private Investigation, Security, Personal Protection and other related fields. There are only a handful of Canadian based groups most are U.S. based. But the information obtained in any Newsgroup is priceless. We have added a few Newsgroups to our "NEWS" page and we will be adding many more in the upcoming weeks so make sure you join all that interest you. There is no cost or obligation to join any of the groups we add to our site.

COMPUTER & INTERNET TOOLS

- Services such as Anonymizer (<http://www.anonymizer.com>) let subscribers hide their IP numbers when surfing the Web. These services encrypt and reroute subscriber's web travels through their proxy servers. This way, sites cannot track a user's information. The cost is around \$4 per month, or less when signing up for a year.
- If you want to know what information you're disclosing to web sites, use Privacy.net's analysis tool(<http://privacy.net/analyze/>). Most people don't worry about disclosing this data, assuming they know about it. So much data is maintained on us that this seems pretty minor. And, other than IP numbers, it isn't personal.

Probably the most known modern day spy is James Bond. The reality is that this very successful fictional spy agent would not last a day in the real world of espionage. Why? A real spy does not drive expensive exotic cars equipped with the latest non-existent spy gadget. Spies rarely if ever carry guns, they're intelligence gatherers not cowboys. James Bond himself is too flashy, he lives a very extrovert lifestyle more like a movie star rather than a spy. A real spy looks like your neighbour, drives a very ordinary car and holds a mundane job in an office building never doing anything that raises questions.



Canadian Private Investigators'
Resource Centre

For General Information: info@cpirc.com

For Membership Information: memberservices@cpirc.com

For Product Information: shop@cpirc.com

For Training Information: training@cpirc.com

For Comments and Opinions: comments@cpirc.com

THANKS TO ALL WHO SUPPORT US!