Risk Management Committee Meeting

YOUR BEST PROTECTION

ACWA JPIA Executive Conference Room
2100 Professional Drive
Roseville, CA 95661

Monday
March 19, 2018
3:00 P.M.

Chairman: David Hodgin, Scotts Valley Water District

Vice Chair: Kathy Tiegs, Cucamonga Valley Water District

Fred Bockmiller, Mesa Water District

Victor Fortenberry, Solano Irrigation District

Ron Kilburg, El Dorado Irrigation District

Bob Kuhn, San Gabriel Basin Water Quality Authority

Gaby Olson, Valley Center Municipal Water District

Tanesha Welch, Madera Irrigation District

Dan York, Sacramento Suburban Water District

RISK MANAGEMENT COMMITTEE MEETING

AGENDA

JPIA Executive Conference Room
2100 Professional Drive, Roseville, CA 95661
(800) 231-5742 - WWW.ACWAJPIA.COM

MONDAY, MARCH 19, 2018, 3:00 P.M.

WEBEX CALL IN: (855) 749-4750; ACCESS CODE: 809 514 226; PASSWORD: 1234
This meeting shall consist of a simultaneous WebEx teleconference call at the ACWA Joint Powers Insurance Authority, 2100 Professional Drive, Roseville, CA 95661 and the following remote sites:

- Kuhn, 400 E Street SW, Washington D.C.
- Kilburg, 2890 Mosquito Road, Placerville

WELCOME

CALL TO ORDER AND ANNOUNCEMENT OF QUORUM

ANNOUNCEMENT RECORDING OF MEETING This meeting may be recorded to assist in preparation of minutes. Recordings will only be kept 30 days following the meeting, as mandated by the California Brown Act.

EVACUATION PROCEDURES

PUBLIC COMMENT Members of the public will be allowed to address the Risk Management Committee on any agenda item prior to the Committee's decision on the item. They will also be allowed to comment on any issues that they wish which may or may not be on the agenda. If anyone present wishes to be heard, please let the Chairman know.

INTRODUCTIONS

ADDITIONS TO OR DELETIONS FROM THE AGENDA

Presenter			Page#
	I.	**CONSENT AGENDA**	
Hodgin	*	A. Approve the minutes of the meeting of May 8, 2017.	**1**
Hodgin		B. Report on meetings attended on behalf of the JPIA.	

Preliminary Agenda-date issued: February 22, 2018
Final Agenda-date issued: March 5, 2018

II. LOSS REPORTS

Sells	*****	A. Review Claims Analysis for the Liability, Property, and Workers' Compensation Programs.	**7**

III. RISK MANAGEMENT

Barake	*	A. Review and provide direction on proposed changes to the H.R. LaBounty Safety Awards Program.	**43**
Barake	*	B. JPIA Source – Risk Management Quarterly Bulletin.	**49**
Barake	*	C. Risk Management Training Update – Course Revisions, Risk Management Regional Training Calendar.	**51**
Barake		D. New Staff Position in Southern California.	**53**
Thesing	*	E. Cyber Security Resources for JPIA Members.	**54**

IV. HUMAN RESOURCES/TRAINING

Slaven	*****	A. Human Resources Update.	**60**
		B. Leadership Program and Training Update.	**62**

V. UPCOMING MEETING(S)

Hodgin		A. There are no additional meetings scheduled for the remainder of the year.	

ADJOURN

*****Related items enclosed.

Americans With Disabilities Act – *The JPIA conforms to the protections and prohibitions contained in Section 202 of the Americans with Disabilities Act of 1990 and the Federal Rules and Regulations adopted in implementation thereof. A request for disability-related modification or accommodation, in order to participate in a public meeting of the JPIA, shall be made to: Terry Lofing, Administrative Assistant II, ACWA JPIA, PO Box 619082, Roseville, CA 95661-9082; telephone (916) 786-5742. The JPIA's normal business hours are Monday – Friday, 7:30 a.m. to 4:30 p.m. (Government Code Section 54954.2, subdivision. (a)(1).)*

Written materials relating to an item on this Agenda that are distributed to the JPIA's Risk Management Committee within 72 hours before it is to consider the item at its regularly scheduled meeting will be made available for public inspection at ACWA JPIA, 2100 Professional Drive, Roseville, CA 95661-3700; telephone (916) 786-5742. The JPIA's normal business hours are Monday – Friday, 7:30 a.m. to 4:30 p.m.

Unapproved Minutes

Risk Management Committee Meeting

Hyatt Regency Monterey
Regency Ballroom 4-6
1 Old Golf Course Road
Monterey, CA 93940
(831) 372-1234

May 8, 2017

MEMBERS PRESENT

Chairman: David T. Hodgin, Scotts Valley Water District
Vice-chair: Brent Hastey, Yuba County Water Agency, ACWA Vice President
Fred Bockmiller, Mesa Water District
Ron Kilburg, El Dorado Irrigation District
Bob Kuhn, San Gabriel Basin Water Quality Authority
Gaby Olson, Valley Center Municipal Water District
Tanesha Welch, Madera Irrigation District
Dan York, Sacramento Suburban Water District

MEMBER ABSENT

Victor Fortenberry, Solano Irrigation District

STAFF PRESENT

Chief Executive Officer/Secretary: Walter "Andy" Sells
Carol Barake, Risk Management Program Manager
Chimene Camacho, HR Coordinator (Recording Secretary)
David deBernardi, Director of Finance
Robert Greenfield, General Counsel
Robin Hudson, Receptionist
Sylvia Robinson, Publications & Web Editor
Patricia Slaven, Director of Administration
Sandra Smith, Employee Benefits Manager
Dianna Sutton, Finance Manager
Karen Thesing, Director of Insurance Services
Bobbette Wells, Executive Assistant to the CEO

OTHERS IN ATTENDANCE

See Attendance List.

WELCOME

Chairman Hodgin welcomed everyone in attendance and introduced the Risk Management Committee members and JPIA staff in attendance.

CALL TO ORDER AND ANNOUNCEMENT OF QUORUM

Chairman Hodgin called the meeting to order at 8:33 a.m. He announced there was a quorum.

ANNOUNCEMENT RECORDING OF MINUTES

Chairman Hodgin announced that the meeting would be recorded to assist in preparation of minutes. Recordings are only kept 30 days following the meeting, as mandated by the California Brown Act.

EVACUATION PROCEDURES

Mr. Sells gave the evacuation procedure instructions.

PUBLIC COMMENT

Chairman Hodgin noted that, as the agenda stated, members of the public would be allowed to address the Risk Management Committee on any agenda item prior to the Committee's decision on that item. Comments on any issues on the agenda, or not on the agenda, were also welcomed. No comments were brought forward.

ADDITIONS TO OR DELETIONS FROM THE AGENDA

Chairman Hodgin asked for any additions to, or deletions from, the agenda; staff had none.

CONSENT AGENDA

Chairman Hodgin called for approval of the minutes of the March 29, 2016 meeting:

> M/S/C (Kuhn/Bockmiller) (Bockmiller-Yes; Hastey-Yes; Kilburg-Yes; Kuhn-Yes; Olson-Yes; Welch-Yes; York-Yes; Hodgin-Yes): That the Risk Management Committee approve the minutes of the March 29, 2016 meeting.

REPORT ON MEETINGS ATTENDED ON BEHALF OF THE JPIA

None reported.

LOSS REPORTS

Review Claims Analysis for the Liability, Property, and Workers' Compensation Programs

Mr. Sells reviewed the claims history for the JPIA's Liability, Property and Workers' Compensation Programs. He presented graphs showing the history of each program by policy year and reported that this year's reports reflect the same trend patterns as past reports. The Liability Program's Self-Insured Retention (SIR) has increased to $5 million for the 2017-18 policy year, as recommended by the Liability Program Committee and approved by the Executive Committee; Mr. Greenfield shared the JPIA received a check from the plaintiff for the Weaverville Community Services District claim; the Property Program reported a higher loss this year due to the Oroville Dam spillway damage; and

the Workers' Compensation Program continues to perform well with no change to the SIR of $2 million.

RISK MANAGEMENT

Risk Management Strategic Planning Recap

Ms. Barake reported on the Risk Management Strategic Planning meeting held on February 9, 2017. Areas discussed included Advisor district re-assignments; review of the Commitment to Excellence (C2E) program; the staff metrics/tracking systems; and training course activities. Ms. Barake summarized the Risk Management team's focus: the C2E and Safety Awards programs, and on-site training alignment with C2E to further reinforce loss control efforts and streamline internal processes.

Risk Management Report Distribution Procedure

Ms. Barake reported on the current report distribution process that has been in place for many years and provided the Committee with a proposal to streamline the process. The new proposal will provide electronic copies (via email) of correspondence for risk assessment surveys, and email confirmations directly from Risk Management Advisors for on-site training delivery.

After providing their input, the Committee agreed that electronic copies of risk assessment survey reports is acceptable. They prefer to continue to receive copies of each of the Risk Assessment reports in a monthly packet, but do not require the email confirmations of on-site trainings to be included.

Safety Awards Program – Commitment to Excellence Categories

Ms. Barake stated that a new field was included on the H.R. LaBounty Safety Awards nomination form to assign each nomination to one of the Commitment to Excellence (C2E) categories. Assigning a C2E category integrates the Safety Awards Program into the Risk Management Department focus on best practices to control losses, especially those related to Vehicle Operations, Construction, Infrastructure and Ergonomics/Falls. At the Spring 2017 Conference, 23 member districts provided 42 award nominations. A list of participating members was included in the 2017 Spring Conference packet.

Training Update – Focus for Risk Management Advisors

The Risk Management Advisors continue to deliver high quality, instructor-led trainings for our members to reinforce best practices and reduce losses. The department delivered 275 classes, with 4,200 participants in fiscal year 2015-16. The trainings focus on water industry best practices rather than regulatory compliance, and offer members the opportunity to provide more effective safety and risk control training. Course content is peer-reviewed and updated on an annual basis.

Ms. Barake presented the list of the most frequently delivered trainings for the past year with the C2E category/loss area related to the training effort. Defensive Driver Training was the number one course, delivered to 51 districts, followed by Traffic Control/Flagger at 28, and Field & Office Ergonomics at 27. A list of additional training topics provided by Risk Management in fiscal year 2015-16 were included in the 2017 Spring

Conference packet. Ms. Barake shared that, at the next Risk Management Department meeting in June, each of the additional risk management training courses will be evaluated.

HUMAN RESOURCES

Training Update

Ms. Slaven shared that the JPIA offers in-person, webinar and online training to its members. The Professional Development Program (PDP) continues to be popular among member agency staff with current enrollment of over one thousand across the three specialties – Human Resources, Supervisor, and Operations. The challenge has been the completion of the specialty for some. JPIA is working to bring additional options to members in order to facilitate greater completions. Overall, the number of staff attending JPIA training whether in-person, online or webinar, continues to increase, as more members take advantage of this added benefit. Training statistics were included in the 2017 Spring Conference packet.

Human Resources Update

Ms. Slaven stated that the JPIA continues to provide members with employment-related support, and training to reduce employment liability claims and encourage a positive work culture. Members in the Liability Program are supported with the Employment Practices Hotline where members can get assistance with employment-related issues, and referral to counsel specializing in employment practices if necessary. Topics range from how to go about hiring someone, the use of sick hours, to dealing with an employee's disability, and everything in between. Open to all members are the Regional Human Resource meetings. Last year, the JPIA delivered one dozen meetings at 11 locations and this year will visit a similar number of regions throughout the state. A list of the meeting locations and dates were included in the 2017 Spring Conference packet.

UPCOMING MEETING(S)

There are no other Risk Management Committee meetings scheduled for 2017.

The Risk Management Committee meeting adjourned at 9:47 a.m.

LIST OF ATTENDEES – RISK MANAGEMENT COMMITTEE MEETING – MAY 8, 2017

District / Organization	*Name*	*Position*
Alameda County Water District	John Weed	Director
Alta Irrigation District	Irma Faria	Alternate Director
Antelope Valley-East Kern Water Agency	Rob Parris	Director
Bella Vista Water District	Jim Smith	Director
Calleguas Municipal Water District	Scott Quady	Director
Carpinteria Valley Water District	Al Orozco	Director
Castaic Lake Water Agency	Jerry Gladbach	Director
Cucamonga Valley Water District	Kathy Tiegs	Director
Donahue Davies, LLP	Kayla Villa	Attorney
El Dorado Irrigation District	Ron Kilburg	Safety/Security Officer
El Dorado Irrigation District	Michael Rafferty	Alternate Director
El Toro Water District	Fred Adjarian	Director
Fresno Irrigation District	George Porter	Director
Fresno Metropolitan Flood Control District	Kendall Groom	Director
Fresno Metropolitan Flood Control District	Alan Hofmann	General Manager
Henry Miller Reclamation District No. 2131	Palmer McCoy	Exec. Assistant
Hi-Desert Water District	Roger Mayes	Director
Humboldt Bay Municipal Water District	John Friedenbach	General Manager
Kings River Conservation District	Randy Shilling	Alternate Director
La Habra Heights County Water District	Pam McVicar	Director
Madera Irrigation District	Carl Janzen	Director
Main San Gabriel Basin Water Master	Dan Arrighi	Director
Mesa Water District	Fred Bockmiller	Director
Mid-Peninsula Water District	Tammy Rudock	General Manager
North Coast County Water District	Jack Burgett	Director
Orange County Water District	Phil Anthony	Director
Orchard Dale Water District	Ed Castaneda	General Manager
Palmdale Water District	Vincent Dino	Alternate Director
Palmdale Water District	Joe Estes	Director
Palmdale Water District	Dennis Lamoreaux	General Manager
Palmdale Water District	Kathy McClaren	Board Member
Palm Ranch Irrigation District	Wayne Nygaard	Director
Paradise Irrigation District	Kevin Phillips	General Manager
Purissima Hills Water District	Robert Anderson	Director
Rancho California Water District	John Hoagland	Director
Rancho California Water District	Eva Plajzer	Asst. General Manager
Rincon Del Diablo Municipal Water District	Greg Thomas	General Manager
Rio Linda/Elverta Community Water District	Paul Green	Director
Rosamond Community Services District	Morrison E. Mackay	Director
Rowland Water District	Tom Coleman	General Manager
Rowland Water District	Robert Lewis	Director
Sacramento Suburban Water District	Mitch Dion	Alternate Director
Sacramento Suburban Water District	Dan York	Asst. General Manager

LIST OF ATTENDEES – RISK MANAGEMENT COMMITTEE MEETING – MAY 8, 2017

District / Organization	*Name*	*Position*
San Bernardino Valley Municipal Water District	Mark Bulot	Director
San Bernardino Valley Municipal Water District	Steve Copelan	Director
San Bernardino Valley Water Conservation District	Milford Harrison	Alternate Director
San Bernardino Valley Water Conservation District	Melody McDonald	Director
San Dieguito Water District	Jace Schwarm	Alternate Director
San Gabriel Basin Water Quality Authority	Jim Byerrum	General Manager
San Gabriel Basin Water Quality Authority	Bob Kuhn	Director
San Gorgonio Pass Water Agency	Leonard Stephenson	Director
Santa Margarita Water District	Kathleen Springer	HR Manager
Scotts Valley Water District	David Hodgin	Director
Solano Irrigation District	Lance Porter	Director
South Coast Water District	Dennis Erdman	Director
South Sutter Water District	Thomas Cuquet	Director
South Tahoe Public Utility District	Shannon Cotulla	Asst. General Manager
South Tahoe Public Utility District	Jim Jones	Director
Sunnyslope County Water District	Judi Johnson	Director
Sweetwater Authority	Jim Smith	General Manager
Tehachapi-Cummings County Water District	Jonathan Hall	Director
Three Valleys Municipal Water District	Brian Bowcock	Director
Upper San Gabriel Valley Municipal Water District	Alfonso Contreras	Director
Vallecitos Water District	Hal Martin	Director
Vallecitos Water District	Tom Scaglione	Asst. General Manager
Valley Center Municipal Water District	Merle Aleshire	Director
Valley Center Municipal Water District	Gaby Olson	Safety Supervisor
Valley Center Municipal Water District	Jim Pugh	Director of Finance
Valley County Water District	Lenet Pacheco	Director
Vista Irrigation District	Paul Dorey	Director
Westborough Water District	Darryl Barrow	General Manager
Westborough Water District	Janet Medina	Director
Western Municipal Water District	S.R. Al Lopez	Director
West Valley Water District	Mike Holmes	General Manager
Yuba County Water Agency	Terri Daly	Admin. Manager
Yuima Municipal Water District	Bill Knutson	Director
Yuima Municipal Water District	Rich Williamson	General Manager

ACWA JPIA
Claims Analysis for the
Liability, Property, and Workers' Compensation Programs
March 19, 2018

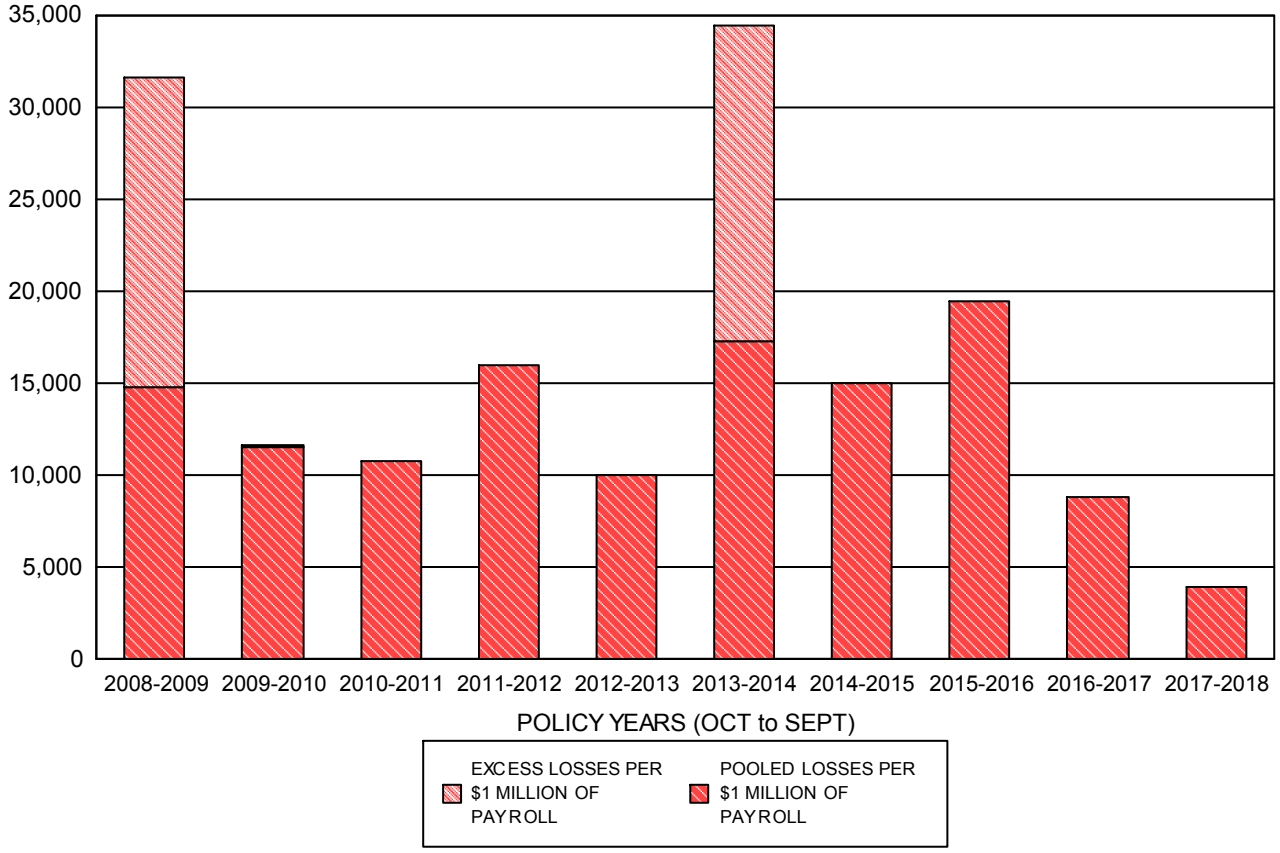
BACKGROUND
The claims history for the JPIA has been very favorable for the past several years. Past reports have included graphs tracking the history of each program by policy year.

CURRENT SITUATION
The current reports reflect the same general trend patterns as past reports. Each program will be reviewed and some of the variances will be discussed.

RECOMMENDATION
None, informational only.

Prepared by: Walter A. Sells, Chief Executive Officer Date prepared: February 22, 2018

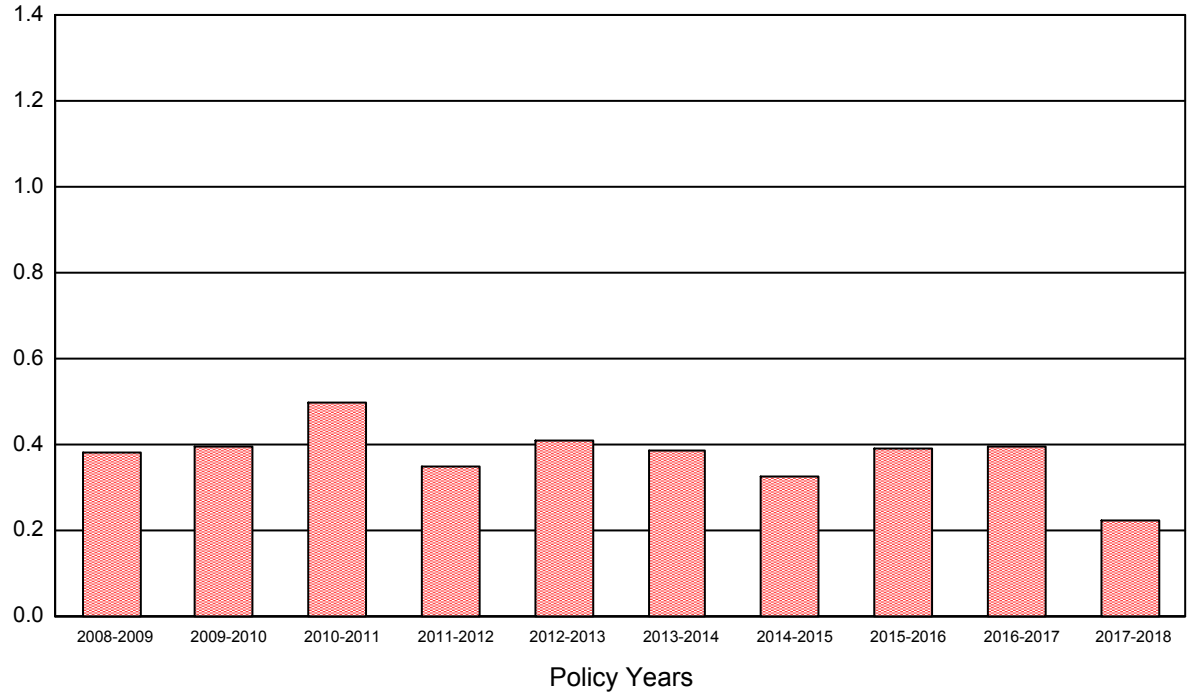
ACWA JPIA - LIABILITY PROGRAM
REPORTED LOSSES PER $1 MILLION OF PAYROLL
FOR MONTH ENDING 2/28/2018



PROGRAM YEAR (10/1)	# OF MEMBERS	SELF INSURED RETENTION	POOLED LOSSES	EXCESS LOSSES	TOTAL LOSSES	ACTUAL PAYROLL	POOLED LOSSES PER $1 MILLION OF PAYROLL	TOTAL LOSSES PER $1 MILLION OF PAYROLL
2003-2004	286	500,000	3,584,119	2,600,000	6,184,119	347,874,665	10,303	17,777
2004-2005	287	500,000	8,889,968	7,420,035	16,310,003	360,896,946	24,633	45,193
2005-2006	286	1,000,000	8,431,860	116,079	8,547,939	380,897,839	22,137	22,442
2006-2007	286	1,000,000	7,373,623	455,000	7,828,623	411,559,778	17,916	19,022
2007-2008	285	1,000,000	3,566,530	0	3,566,530	436,649,863	8,168	8,168
2008-2009	284	1,000,000	6,432,507	7,365,359	13,797,866	435,872,180	14,758	31,656
2009-2010	285	1,000,000	5,125,418	49,508	5,174,926	445,710,401	11,499	11,611
2010-2011	286	1,000,000	4,856,047	0	4,856,047	451,207,328	10,762	10,762
2011-2012	292	2,000,000	7,364,188	0	7,364,188	459,712,593	16,019	16,019
2012-2013	293	2,000,000	4,675,831	0	4,675,831	467,699,841	9,998	9,998
2013-2014	291	2,000,000	8,396,084	8,280,024	16,676,107	484,457,504	17,331	34,422
2014-2015	292	2,000,000	7,489,050	0	7,489,050	499,915,511	14,981	14,981
2015-2016	294	2,000,000	10,108,358	0	10,108,358	520,745,561	19,411	19,411
2016-2017	303	5,000,000	4,891,280	0	4,891,280	553,052,844	8,844	8,844
2017-2018	312	5,000,000	947,385	0	947,385	570,578,305	3,985	3,985

- Latest Policy Year's 'Losses' include partial activity.
- Latest Policy Year's 'Losses Per $1 Million of Payroll' have been annualized using 5 months data.

ACWA JPIA - LIABILITY PROGRAM
OCCURRENCES PER $1 MILLION OF PAYROLLS REPORT
FOR MONTH ENDING 2/28/2018



PROGRAM YEAR (10/1)	NUMBER OF OCCUR	ACTUAL PAYROLLS	HISTORICAL INCREASE	INFLATION ADJUSTMENT FACTOR	INFLATION ADJUSTED PAYROLLS	# OF OCCURRENCES PER $1 MILLION OF INFLATION ADJUSTED PAYROLLS
2003-2004	281	347,874,665	2.2%	1.326	461,167,077.21	0.61
2004-2005	305	360,896,946	4.1%	1.297	468,131,435.04	0.65
2005-2006	279	380,897,839	3.0%	1.246	474,616,003.19	0.59
2006-2007	252	411,559,778	2.5%	1.210	497,885,603.17	0.51
2007-2008	228	436,649,863	4.3%	1.180	515,354,539.99	0.44
2008-2009	189	435,872,180	0.0%	1.132	493,227,883.72	0.38
2009-2010	199	445,710,401	0.0%	1.132	504,360,699.71	0.39
2010-2011	254	451,207,328	0.5%	1.132	510,580,958.10	0.50
2011-2012	181	459,712,593	3.5%	1.126	517,617,330.49	0.35
2012-2013	207	467,699,841	2.2%	1.088	508,802,551.82	0.41
2013-2014	199	484,457,504	1.3%	1.064	515,687,791.20	0.39
2014-2015	172	499,915,511	2.0%	1.051	525,313,218.90	0.33
2015-2016	209	520,745,561	1.0%	1.030	536,472,076.83	0.39
2016-2017	222	553,052,844	2.0%	1.020	564,113,900.79	0.39
2017-2018	53	570,578,305	2.9%	1.000	570,578,305.29	0.22

- Latest Policy Year's 'Number of Occur' include partial activity.
- Latest Policy Year's '# Of Occurrences Per $1 Million of Inflation Adjusted Payrolls' has been annualized using 5 months data.
- Payrolls Adjusted for Inflation - CNP's Omitted - Small Claims Included.
- Factor based on CPI for West Coast from US Dept of Labor

ACWA JPIA - LIABILITY PROGRAM
SIGNIFICANT LARGE CLAIMS (IN MILLIONS)
FOR MONTH ENDING 2/28/2018

CLAIM NUMBER	LOSS DATE	DISTRICT	DESCRIPTION	STATUS	LOSS AMOUNT
POLICY YEAR 1982-1983		**SELF INSURED RETENTION**	**500,000**		
045137	03/01/1983	Arvin-Edison Water Storage District	Flooding	Closed	3.1
037514	03/01/1983	Kern Delta Water District	Flooding as a result of canal bank break	Closed	0.6
				TOTAL	**3.7**
POLICY YEAR 1984-1985		**SELF INSURED RETENTION**	**500,000**		
051301	12/01/1984	Ramona Municipal Water District	Reparian rights dispute over water storage in reservoir	Closed	0.8
052420	05/17/1985	Ramona Municipal Water District	Construction dispute with contractor	Closed	0.9
				TOTAL	**1.7**
POLICY YEAR 1985-1986		**SELF INSURED RETENTION**	**500,000**		
040892	02/18/1986	American River Flood Control District	Flooding as a result of heavy rainfall	Closed	1.0
059596	04/01/1986	San Bernardino Valley Water Conservation District	City owned streets damaged by recharge operations	Closed	4.4
040275	03/01/1986	Westlands Water District	District's failure to provide tailwater drainage resulted in damage to crops	Closed	0.5
				TOTAL	**5.8**
POLICY YEAR 1986-1987		**SELF INSURED RETENTION**	**1,000,000**		
063825	08/25/1987	Rancho California Water District	District groundwater pumping operations damaged property	Closed	4.7
				TOTAL	**4.7**
POLICY YEAR 1987-1988		**SELF INSURED RETENTION**	**500,000**		
029044	07/28/1988	Desert Water Agency	Auto accident with 3 people seriously injured	Closed	1.4
047976	02/22/1988	Kern Delta Water District	Herbicide overspray damaged crops	Closed	1.0
067446	06/15/1988	Trabuco Canyon Water District	Negligent administration resulted in personal injury	Closed	0.9
				TOTAL	**3.4**
POLICY YEAR 1988-1989		**SELF INSURED RETENTION**	**500,000**		
057674	10/01/1988	Fallbrook Public Utility District	Flooding as result of improper maintenance of valve	Closed	0.5
049235	08/09/1989	Friant Water Users Authority	Auto accident forced claimant vehicle into canal severe injury to driver	Closed	1.1
				TOTAL	**1.6**
POLICY YEAR 1989-1990		**SELF INSURED RETENTION**	**500,000**		
001026	05/26/1990	Montecito Water District	Flooding as a result of diversion of rainfall runoff by District facilities	Closed	1.3
057798	03/01/1990	Rainbow Municipal Water District	District's failure to supply sewer service resulted in diminished property values	Closed	1.0
				TOTAL	**2.3**

ACWA JPIA - LIABILITY PROGRAM
SIGNIFICANT LARGE CLAIMS (IN MILLIONS)
FOR MONTH ENDING 2/28/2018

CLAIM NUMBER	LOSS DATE	DISTRICT	DESCRIPTION	STATUS	LOSS AMOUNT
POLICY YEAR 1990-1991		**SELF INSURED RETENTION**	**500,000**		
100586	02/25/1991	Elsinore Valley Municipal Water District	Flooding of vacant land as a result of water releases by District	Closed	0.6
100345	10/01/1990	Vandenberg Village Community Services District	Contaminated water	Closed	0.6
				TOTAL	**1.2**
POLICY YEAR 1992-1993		**SELF INSURED RETENTION**	**500,000**		
101220	01/16/1993	Rancho California Water District	Flooding as a result of water main line break	Closed	0.6
100929	01/09/1993	Yorba Linda Water District	Flooding as a result of water main line break	Closed	1.2
				TOTAL	**1.9**
POLICY YEAR 1993-1994		**SELF INSURED RETENTION**	**500,000**		
101883	08/29/1994	Alta Irrigation District	Seepage from District canal damaged orchards	Closed	2.0
101638	01/25/1994	North of the River Municipal Water District	Wrongful termination based upon age discrimination	Closed	0.7
				TOTAL	**2.6**
POLICY YEAR 1994-1995		**SELF INSURED RETENTION**	**500,000**		
96-2270	08/25/1995	ACWA/JPIA	Wrongful termination based upon alleged retaliation	Closed	5.4
102462	03/10/1995	Fresno Irrigation District	Flooding as a result of rainfall runoff backing up behind District canal banks	Closed	1.0
102170	04/10/1995	Kings River Conservation District	Flooding as a result of canal bank break	Closed	1.0
102729	03/30/1995	Las Virgenes Municipal Water District	Flooding as a result of water main line break caused by landslide	Closed	0.6
102314	06/10/1995	Madera Irrigation District	Seepage from canal damaged orchard	Closed	0.9
102240	05/17/1995	Walnut Valley Water District	Landslide allegedly caused by leaks from District main lines damaged homes	Closed	0.7
				TOTAL	**9.6**
POLICY YEAR 1995-1996		**SELF INSURED RETENTION**	**500,000**		
102934	05/23/1996	Elsinore Valley Municipal Water District	Water pipe leak damaged sand reserve	Closed	4.8
102728	12/13/1995	Kern Delta Water District	District headwall allowed rainfall to backup onto road contributing to the cause of an auto accident	Closed	1.5
97-3781	12/17/1995	Las Virgenes Municipal Water District	Wrongful termination based upon alleged racial discrimination and retaliation	Closed	0.7
				TOTAL	**7.0**
POLICY YEAR 1996-1997		**SELF INSURED RETENTION**	**500,000**		
103075	01/26/1997	Crestline Village Water District	Flooding as a result of water main line break	Closed	0.7
				TOTAL	**0.7**

ACWA JPIA - LIABILITY PROGRAM
SIGNIFICANT LARGE CLAIMS (IN MILLIONS)
FOR MONTH ENDING 2/28/2018

CLAIM NUMBER	LOSS DATE	DISTRICT	DESCRIPTION	STATUS	LOSS AMOUNT
POLICY YEAR 1997-1998		**SELF INSURED RETENTION**	**500,000**		
99-1171	06/24/1998	Elsinore Valley Municipal Water District	Wrongful termination based upon alleged retaliation	Closed	0.6
103686	04/10/1998	Las Virgenes Municipal Water District	Landslide allegedly caused by leaks from District main lines damaged homes	Closed	2.4
103621	01/15/1998	Merced Irrigation District	Claimants allege District facilities contributing to flooding around their property	Closed	1.7
				TOTAL	**4.8**
POLICY YEAR 1998-1999		**SELF INSURED RETENTION**	**500,000**		
00-1986	09/15/1999	Fresno Metropolitan Flood Control District	Auto accident with two serious injuries	Closed	0.9
99-1603	02/17/1999	Tahoe City Public Utility District	Sewer backup damaged restaurant and well	Closed	0.7
				TOTAL	**1.6**
POLICY YEAR 1999-2000		**SELF INSURED RETENTION**	**500,000**		
01-3179	01/01/2000	Santa Clarita Valley Water Agency	District sued several corporations for contamination of its aquifer. The corporations sued the District claiming that the District caused the contamination.	Closed	1.0
				TOTAL	**1.0**
POLICY YEAR 2001-2002		**SELF INSURED RETENTION**	**500,000**		
02-4265	06/07/2002	El Toro Water District	District mainline leaked water onto road contributing to cause of auto accident one serious injury	Closed	0.8
				TOTAL	**0.8**
POLICY YEAR 2002-2003		**SELF INSURED RETENTION**	**500,000**		
03-4901	02/10/2003	Camrosa Water District	Flooding as a result of water main line break	Closed	0.6
04-5381	01/21/2003	Rainbow Municipal Water District	Wrongful termination as a result of alleged retaliation	Closed	0.6
				TOTAL	**1.2**
POLICY YEAR 2003-2004		**SELF INSURED RETENTION**	**500,000**		
04-5607	10/09/2003	Citrus Heights Water District	Serious injury as a result of using District air bleed-off valve	Closed	3.1
				TOTAL	**3.1**

ACWA JPIA - LIABILITY PROGRAM
SIGNIFICANT LARGE CLAIMS (IN MILLIONS)
FOR MONTH ENDING 2/28/2018

CLAIM NUMBER	LOSS DATE	DISTRICT	DESCRIPTION	STATUS	LOSS AMOUNT
POLICY YEAR 2004-2005		**SELF INSURED RETENTION**	**500,000**		
06-7432	07/28/2005	Goleta Water District	Auto accident District driver hit bicyclist	Closed	0.9
06-7603	05/25/2005	Merced Irrigation District	A 4 year old boy fell into a District owned canal and drowned.	Closed	0.5
07-8252	09/11/2005	Palmdale Water District	Smith rendered quadriplegic as a result of auto accident at District job site.	Closed	0.5
08-9758	01/01/2005	Santa Clarita Valley Water Agency	Plntff contends that swale cut on District property above plntff's property caused rainfall runoff to travel downhil and damage the slope of plntff's property.	Closed	0.5
05-7191	05/16/2005	South Coast Water District	Landslide allegedly caused by leaks from District main lines damaged homes	Closed	6.9
05-7225	05/26/2005	Tulare Irrigation District	Flooding as a result of a break in berm damaged private property	Closed	1.0
06-7456	03/01/2005	Yorba Linda Water District	Clmnt alleges seepage from District water line trench caused a landslide that damaged his house.	Closed	0.5
				TOTAL	**10.8**
POLICY YEAR 2005-2006		**SELF INSURED RETENTION**	**1,000,000**		
06-8065	04/20/2006	Arvin-Edison Water Storage District	Flooding as a result of a break in berm damaged private property	Closed	0.8
06-8142	04/03/2006	Merced Irrigation District	Grimes canal broke during storm even and flooded numerous homes.	Closed	1.1
06-7929	12/09/2005	North Yuba Water District	Clmnt contends that he was wrongfully terminated from his job as District GM	Closed	1.0
06-8199	06/18/2006	Orchard Dale Water District	Flooding as a result of water main line break	Closed	0.5
13-0458	03/01/2006	Rancho California Water District	Contends soil contamination causing illness, etc.	Closed	0.5
06-7817	01/25/2006	Sweetwater Authority	Flooding as a result of water main line break	Closed	1.0
				TOTAL	**5.0**
POLICY YEAR 2006-2007		**SELF INSURED RETENTION**	**1,000,000**		
09-0113	06/27/2007	Merced Irrigation District	Clmnt filed EPL claim with District in which he alleges racial discrimination and retaliation.	Closed	1.5
				TOTAL	**1.5**
POLICY YEAR 2007-2008		**SELF INSURED RETENTION**	**1,000,000**		
09-0563	07/15/2008	San Luis & Delta-Mendota Water Authority	Clmnt was driving a truck on the District's canal bank road. She ran a STOP sign at the intersection of the canal bank road and a main road and was struck by a truck. Both trucks went into the District canal and all occupants died.	Closed	1.0
				TOTAL	**1.0**

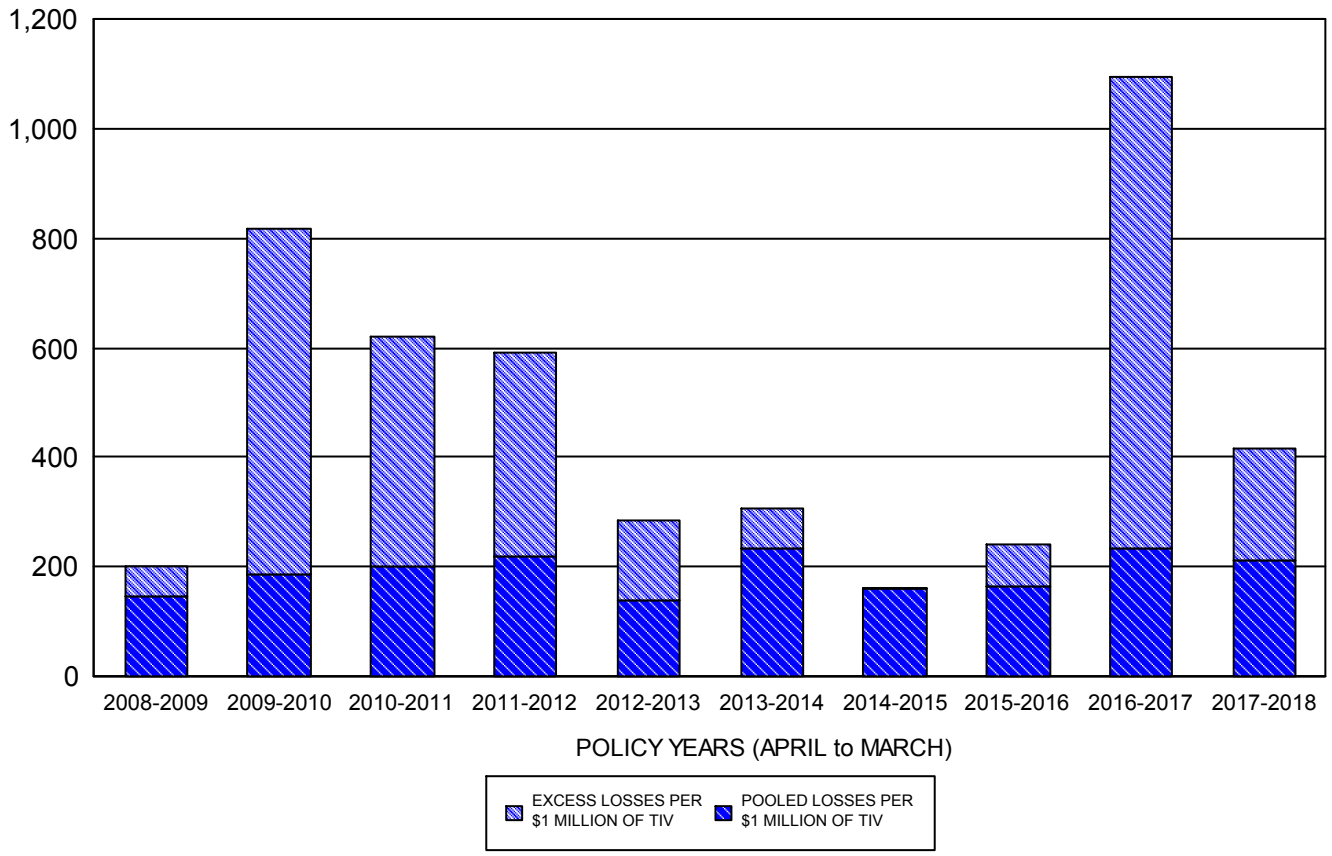
ACWA JPIA - LIABILITY PROGRAM
SIGNIFICANT LARGE CLAIMS (IN MILLIONS)
FOR MONTH ENDING 2/28/2018

CLAIM NUMBER	LOSS DATE	DISTRICT	DESCRIPTION	STATUS	LOSS AMOUNT
POLICY YEAR 2008-2009		**SELF INSURED RETENTION**	**1,000,000**		
09-0704	04/06/2009	Oakdale Irrigation District	District vehicle hit claimant in street	Closed	0.6
10-1108	08/20/2009	Walnut Valley Water District	Vehicle lost control and hit fire hydrant & light pole	Closed	0.9
09-0419	11/15/2008	Yorba Linda Water District	Houses damaged by fire. Allegations against the District is that there wasn't enough water pressure to fire hydrants.	Closed	8.4
				TOTAL	**9.9**
POLICY YEAR 2009-2010		**SELF INSURED RETENTION**	**1,000,000**		
10-1565	02/25/2010	Merced Irrigation District	EPL claim	Closed	1.0
				TOTAL	**1.0**
POLICY YEAR 2010-2011		**SELF INSURED RETENTION**	**1,000,000**		
12-0096	10/01/2010	Alta Irrigation District	Clmnt contends that water leaking from District canal damaged his vineyard, house and well.	Closed	0.9
				TOTAL	**0.9**
POLICY YEAR 2011-2012		**SELF INSURED RETENTION**	**2,000,000**		
14-0046	07/01/2012	Central Basin Municipal Water District	Clmnt contends that a member of the District Board of Directors sexually harrassed her and canceled her contract with the District in retaliation for her rebuffing the sexual advances.	Closed	0.7
12-0664	02/09/2012	Fallbrook Public Utility District	Main line break sent water into local high school	Closed	0.6
13-0251	08/13/2012	Rancho California Water District	Clmnt contends that the District misclassified his job as an Independent Contractor when he was really a District employee.	Open	1.3
				TOTAL	**2.6**
POLICY YEAR 2012-2013		**SELF INSURED RETENTION**	**2,000,000**		
13-0376	12/19/2012	Friant Water Authority	Claimant's husband stepped in front o oncoming District truck	Closed	0.8
				TOTAL	**0.8**
POLICY YEAR 2013-2014		**SELF INSURED RETENTION**	**2,000,000**		
17-0483	03/27/2014	Oakdale Irrigation District	Failure to accommodate, retaliation and wrongful termination	Open	0.5
14-0227	10/15/2013	Santa Fe Irrigation District	8" main broke flooding homes	Closed	1.1
14-0779	05/19/2014	Semitropic Water Storage District	Herbicide drift	Open	10.3
15-0301	05/15/2014	Vallecitos Water District	Claimants allege fire hydrants were nc operational, which allowed homes to burn down during Cocos Fire.	Closed	0.5
				TOTAL	**12.5**

ACWA JPIA - LIABILITY PROGRAM
SIGNIFICANT LARGE CLAIMS (IN MILLIONS)
FOR MONTH ENDING 2/28/2018

CLAIM NUMBER	LOSS DATE	DISTRICT	DESCRIPTION	STATUS	LOSS AMOUNT
POLICY YEAR 2014-2015		**SELF INSURED RETENTION**	**2,000,000**		
15-0394	12/12/2014	Corcoran Irrigation District	District vehicle attempted to make a U-turn in front of claimant vehicle	Open	1.7
15-0245	10/16/2014	Santa Clarita Valley Water Agency	14" high pressure line broke sending water into claimants homes	Closed	0.9
15-0329	11/30/2014	Serrano Water District	Pipeline break, water flooded residence	Open	0.8
				TOTAL	**3.4**
POLICY YEAR 2015-2016		**SELF INSURED RETENTION**	**2,000,000**		
16-0661	04/04/2016	Fresno Irrigation District	Claimant alleges canal broke, flooding his almond orchard and created damages to trees and future crops.	Open	1.2
16-0373	12/13/2015	Purissima Hills Water District	Water main break sending water into large basement living area.	Closed	1.6
17-0726	07/15/2016	Rowland Water District	Discrimination and termination based upon age and disability	Open	0.5
17-0113	06/30/2016	Upper San Gabriel Valley Municipal Water District	Sexual Harassment	Closed	0.6
17-0366	08/24/2016	West Valley Water District	Clmt alleges wrongful termination.	Open	0.7
				TOTAL	**4.5**
POLICY YEAR 2016-2017		**SELF INSURED RETENTION**	**5,000,000**		
17-0332	12/09/2016	Calleguas Municipal Water District	District line break sent water into claimant's home	Open	0.6
18-0023	03/25/2017	Kirkwood Meadows Public Utility District	Clmt alleges District's propane system malfunctioned, which caused explosion and loss of home.	Open	0.9
17-0733	06/02/2017	Mid-Peninsula Water District	District main break sent water & mud into/onto claimants properties	Open	0.6
				TOTAL	**2.1**

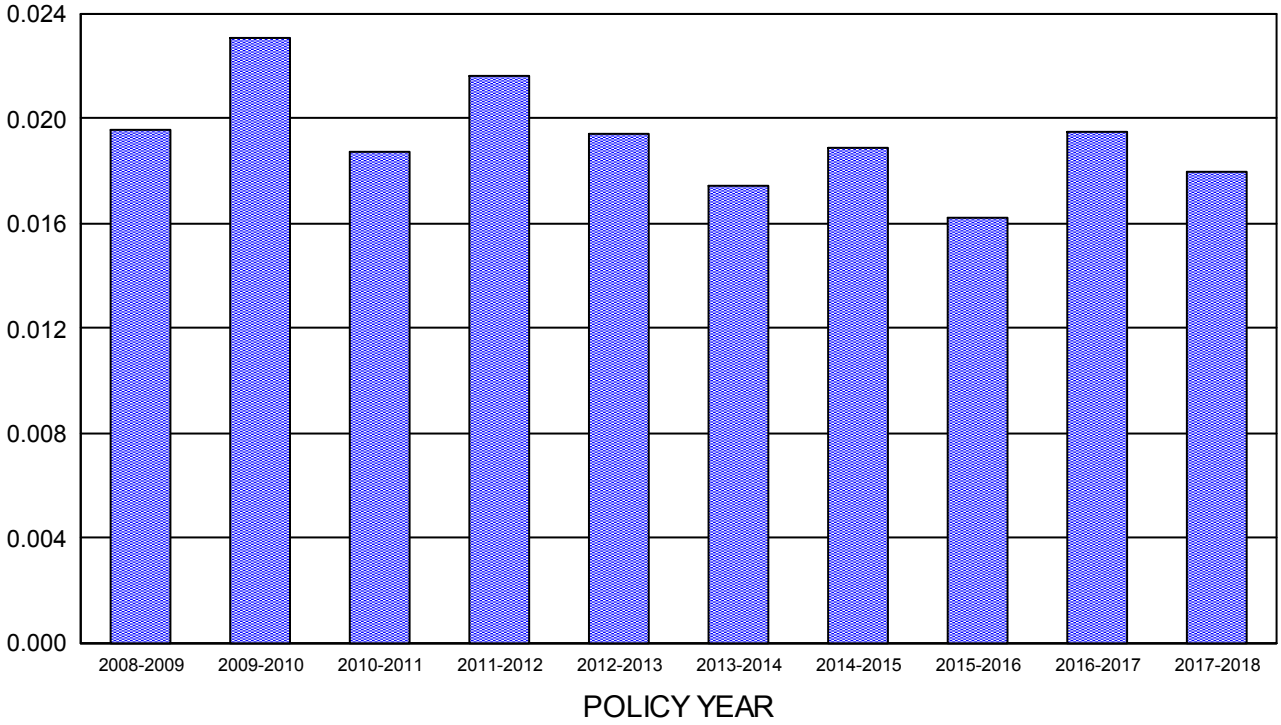
ACWA JPIA - PROPERTY PROGRAM
REPORTED LOSSES PER $1 MILLION OF INSURED VALUES
FOR MONTH ENDING 2/28/2018



POLICY YEAR (4/1)	TOTAL INSURED VALUES	SELF INSURED RETENTION	POOLED LOSSES	EXCESS LOSSES	INCURRED LOSSES	POOLED LOSSES PER $1 MILLION OF VALUES	TOTAL LOSSES PER $1 MILLION OF VALUES
2003-2004	2,085,410,030	50,000	611,837	962,625	1,574,462	293	755
2004-2005	2,298,049,283	50,000	677,023	616,127	1,293,149	295	563
2005-2006	2,574,260,780	50,000	553,692	364,480	918,173	215	357
2006-2007	2,771,109,403	50,000	734,498	1,864,119	2,598,617	265	938
2007-2008	3,264,683,172	50,000	696,768	1,375,733	2,072,501	213	635
2008-2009	3,463,259,945	50,000	512,340	189,526	701,866	148	203
2009-2010	3,717,811,097	50,000	689,081	2,355,173	3,044,254	185	819
2010-2011	4,011,837,238	50,000	801,074	1,693,574	2,494,649	200	622
2011-2012	4,232,136,308	50,000	922,930	1,585,784	2,508,715	218	593
2012-2013	4,486,160,745	50,000	615,618	657,678	1,273,296	137	284
2013-2014	4,737,842,030	100,000	1,107,753	342,512	1,450,265	234	306
2014-2015	4,992,972,478	100,000	801,718	7,727	809,445	161	162
2015-2016	5,245,191,402	100,000	871,272	398,104	1,269,376	166	242
2016-2017	5,474,115,750	100,000	1,289,402	4,705,646	5,995,048	236	1,095
2017-2018	6,129,845,103	100,000	1,187,051	1,161,275	2,348,326	211	418

- Latest Policy Year's 'Losses' include partial activity.
- Latest Policy Year's 'Losses Per $1 Million of Values' has been annualized using 11 months data.

ACWA JPIA - PROPERTY PROGRAM
OCCURRENCES PER $1 MILLION OF INSURED VALUES
FOR MONTH ENDING 2/28/2018



PROGRAM YEAR (4/1)	NUMBER OF OCCUR	TOTAL INSURED VALUES (TIV)	INFLATION ADJUSTMENT ANNUAL %	INFLATION ADJUSTMENT FACTOR	INFLATION ADJUSTED TIV	# OF OCCURRENCES PER $1 MILLION OF INFLATION ADJUSTED TOTAL INSURED VALUES
2003-2004	96	2,085,410,030	1.90	1.355	2,826,167,726	0.0340
2004-2005	90	2,298,049,283	3.30	1.330	3,056,269,368	0.0294
2005-2006	83	2,574,260,780	3.40	1.287	3,314,244,232	0.0250
2006-2007	90	2,771,109,403	3.30	1.245	3,450,365,497	0.0261
2007-2008	117	3,264,683,172	3.50	1.205	3,935,067,164	0.0297
2008-2009	79	3,463,259,945	0.00	1.165	4,033,256,561	0.0196
2009-2010	100	3,717,811,097	1.50	1.165	4,329,702,719	0.0231
2010-2011	86	4,011,837,238	3.00	1.147	4,603,074,690	0.0187
2011-2012	102	4,232,136,308	2.10	1.114	4,714,407,716	0.0216
2012-2013	95	4,486,160,745	1.30	1.091	4,894,592,955	0.0194
2013-2014	89	4,737,842,030	1.80	1.077	5,102,850,923	0.0174
2014-2015	100	4,992,972,478	1.00	1.058	5,282,551,001	0.0189
2015-2016	89	5,245,191,402	1.80	1.048	5,494,453,388	0.0162
2016-2017	110	5,474,115,750	2.90	1.029	5,632,865,107	0.0195
2017-2018	101	6,129,845,103	0.00	1.000	6,129,845,103	0.0180

- Latest Policy Year's 'Number of Occur' include partial activity.
- Latest Policy Year's '# of Occurrences Per $1 Million of Inflation Adjusted Total Insured Values' has been annualized using 11 months data.

ACWA JPIA - PROPERTY PROGRAM
SIGNIFICANT LARGE CLAIMS OVER $75,000
FOR MONTH ENDING 2/28/2018

CLAIM NUMBER	LOSS DATE	DISTRICT	DESCRIPTION	STATUS	LOSS AMOUNT	POLICY YEAR TOTAL
POLICY YEAR	**1987-1988**					
87011	08/11/1987	Glenn-Colusa Irrigation District	Fire destroyed shop building	Closed	100,592	
87020	10/22/1987	Yuima Municipal Water District	Mudslide damaged building	Closed	145,322	
			POLICY YEAR 1987-1988		**245,914**	**505,530**
POLICY YEAR	**1989-1990**					
89011	07/14/1989	Central California Irrigation District	Fire destroyed building	Closed	100,259	
			POLICY YEAR 1989-1990		**100,259**	**292,058**
POLICY YEAR	**1991-1992**					
91035	06/10/1991	Oakdale Irrigation District	Vandals damaged canal	Closed	85,250	
			POLICY YEAR 1991-1992		**85,250**	**237,995**
POLICY YEAR	**1992-1993**					
92017	08/22/1992	Ramona Municipal Water District	Seam on water tank cover split	Closed	260,474	
92015	08/17/1992	South Coast Water District	Garage and shop destroyed by fire	Closed	223,359	
			POLICY YEAR 1992-1993		**483,833**	**687,046**
POLICY YEAR	**1995-1996**					
95006	05/24/1995	San Diego County Water Authority	Mudslide damaged control room.	Closed	94,729	
			POLICY YEAR 1995-1996		**94,729**	**262,843**
POLICY YEAR	**1996-1997**					
96057	11/26/1996	East Orange County Water District	Wind damaged reservoir roof	Closed	113,898	
96072	02/15/1997	Lower Tule River Irrigation District	Capacitor fire resulted in business interruption claim	Closed	75,860	
96032	08/11/1996	Semitropic Water Storage District	Turbine flooded during power outage	Closed	75,495	
96028	08/06/1996	Valley Center Municipal Water District	Power surge damaged electrical panel	Closed	127,265	
			POLICY YEAR 1996-1997		**392,518**	**591,187**

ACWA JPIA - PROPERTY PROGRAM
SIGNIFICANT LARGE CLAIMS OVER $75,000
FOR MONTH ENDING 2/28/2018

CLAIM NUMBER	LOSS DATE	DISTRICT	DESCRIPTION	STATUS	LOSS AMOUNT	POLICY YEAR TOTAL
POLICY YEAR		**1997-1998**				
97001	04/02/1997	East Orange County Water District	Wind damaged reservoir roof	Closed	85,535	
97015	07/03/1997	Elsinore Valley Municipal Water District	Fire damaged building	Closed	94,483	
97050	10/04/1997	Orange County Water District	Power surge damaged electrical panel	Closed	89,851	
97035	08/31/1997	Reclamation District #108	Fire damaged building	Closed	263,928	
			POLICY YEAR 1997-1998		**533,798**	**1,067,247**
POLICY YEAR		**1998-1999**				
99-1633	01/15/1999	Madera-Chowchilla Water and Power Authority	Hydro generator down	Closed	181,786	
98002	04/09/1998	Palmdale Water District	Water backed up into water treatment plant	Closed	176,027	
98008	04/22/1998	Wheeler Ridge-Maricopa Water Storage District	Fire damaged building	Closed	149,666	
			POLICY YEAR 1998-1999		**507,478**	**959,743**
POLICY YEAR		**1999-2000**				
99-1771	06/13/1999	Madera-Chowchilla Water and Power Authority	Hydro-electric plant turbine sustained damage of unknown origin.	Closed	155,095	
00-2212	12/29/1999	Rancho California Water District	Fire damaged building and contents	Closed	80,822	
			POLICY YEAR 1999-2000		**235,916**	**623,868**
POLICY YEAR		**2000-2001**				
01-2850	10/10/2000	Arvin-Edison Water Storage District	Fire damaged a pump motor	Closed	151,567	
01-2747	09/01/2000	Bella Vista Water District	Lightning strike damaged transformer	Closed	123,113	
01-3162	02/26/2001	Santa Clarita Valley Water Agency	Water leaked into ozone output line, flooding 2 ozone generator units.	Closed	202,400	
01-2770	09/11/2000	Yorba Linda Water District	Toilet backed up in District office	Closed	146,176	
			POLICY YEAR 2000-2001		**623,256**	**1,203,199**

ACWA JPIA - PROPERTY PROGRAM
SIGNIFICANT LARGE CLAIMS OVER $75,000
FOR MONTH ENDING 2/28/2018

CLAIM NUMBER	LOSS DATE	DISTRICT	DESCRIPTION	STATUS	LOSS AMOUNT	POLICY YEAR TOTAL
POLICY YEAR		**2002-2003**				
02-4208	04/25/2002	Kern Water Bank Authority	Lightning strike damaged 3 recovery wells and pump station	Closed	81,348	
03-4395	08/02/2002	Madera-Chowchilla Water and Power Authority	Plant shutdown - cause - unknown.	Closed	1,321,842	
			POLICY YEAR 2002-2003		**1,403,190**	**2,056,172**
POLICY YEAR		**2003-2004**				
03-5189	05/22/2003	Berrenda Mesa Water District	2000 HP motor & control switch was damaged due to PG&E interruption	Closed	76,488	
04-5514	08/01/2003	Friant Power Authority	Fire damaged electrical panel and resulted in business interruption claim	Closed	386,149	
04-5662	10/28/2003	Helix Water District	Fire damaged residential building and garage	Closed	380,036	
04-6013	02/26/2004	Mountain Gate Community Services District	Hail damaged the District office	Closed	79,895	
			POLICY YEAR 2003-2004		**922,568**	**1,574,462**
POLICY YEAR		**2004-2005**				
05-6526	09/04/2004	Calaveras County Water District	Fire damaged District's "602" tank	Closed	205,341	
05-6805	12/20/2004	Cucamonga Valley Water District	Fire damaged control panel	Closed	107,938	
05-6398	07/21/2004	Merced Irrigation District	Vandalism to heavy equipment	Closed	111,928	
05-6378	07/16/2004	Serrano Water District	District pump failed - damage to pump and control panel.	Closed	111,340	
04-6239	06/11/2004	Stockton-East Water District	Fire damaged control panel	Closed	153,314	
05-6797	12/19/2004	Western Canal Water District	Water/sewage backed up into ice maker drain - flooded office	Closed	77,337	
			POLICY YEAR 2004-2005		**767,198**	**1,293,149**
POLICY YEAR		**2005-2006**				
07-8600	03/01/2006	American River Flood Control District	District employee embezzled funds from District.	Closed	104,221	
06-7661	11/15/2005	Mission Hills Community Services District	Fire damaged building	Closed	235,885	
06-7741	12/22/2005	North Coast County Water District	Fire damaged vactor truck	Closed	124,057	
06-7777	12/22/2005	Reclamation District #108	Electrical short damaged pump motor	Closed	82,134	
			POLICY YEAR 2005-2006		**546,297**	**918,173**

ACWA JPIA - PROPERTY PROGRAM
SIGNIFICANT LARGE CLAIMS OVER $75,000
FOR MONTH ENDING 2/28/2018

CLAIM NUMBER	LOSS DATE	DISTRICT	DESCRIPTION	STATUS	LOSS AMOUNT	POLICY YEAR TOTAL
POLICY YEAR	**2006-2007**					
07-8416	09/07/2006	Arvin-Edison Water Storage District	Fire damaged building	Closed	194,849	
07-8725	01/14/2007	Golden Hills Community Services District	Fire sprinkler line broke & flooded office	Closed	145,348	
07-8891	03/19/2007	San Diego County Water Authority	Flood damaged hydroelectric plant when two water supply lines ruptured	Closed	1,575,000	
			POLICY YEAR 2006-2007		**1,915,197**	**2,598,617**
POLICY YEAR	**2007-2008**					
08-9455	10/22/2007	Fallbrook Public Utility District	Rice Canyon Fire burned 2 chlorine stations	Closed	968,918	
08-9450	10/26/2007	Helix Water District	Fire destroyed caretaker's residence @ diversion dam.	Closed	180,404	
07-9107	06/05/2007	San Luis Water District	Fire damaged residence	Closed	104,129	
08-9424	10/12/2007	Yolo County Flood Control & Water Conservation District	Fire destroyed Hunting Lodge rental	Closed	145,809	
			POLICY YEAR 2007-2008		**1,399,260**	**2,072,501**
POLICY YEAR	**2008-2009**					
09-0508	10/01/2008	Merced Irrigation District	Rented boomlift rolled	Closed	98,959	
			POLICY YEAR 2008-2009		**98,959**	**701,866**
POLICY YEAR	**2009-2010**					
10-0956	05/07/2009	Cachuma Operation and Maintenance Board	Fire damaged Core Shed	Closed	312,035	
10-1202	05/28/2009	Calleguas Municipal Water District	Boiler & Machinery - Well #12	Closed	90,084	
13-0295	10/30/2009	Calleguas Municipal Water District	B&M - Well #10	Closed	135,715	
13-0307	09/04/2009	Calleguas Municipal Water District	B&M - Well 9	Closed	198,902	
13-0309	08/31/2009	Calleguas Municipal Water District	B&M - Well 16	Closed	122,111	
10-1458	02/15/2010	Kanawha Water District	Fire damaged shop	Closed	440,577	
10-1495	11/07/2009	Merced Irrigation District	Contractor dropped washer into 100 MVA transformer	Closed	1,032,000	
10-1650	03/12/2010	Mission Springs Water District	Employee embezzeled funds.	Open	99,460	
10-1143	09/20/2009	West Basin Municipal Water District	Water damaged building due to pump failure	Closed	108,275	
			POLICY YEAR 2009-2010		**2,539,159**	**3,044,254**

ACWA JPIA - PROPERTY PROGRAM
SIGNIFICANT LARGE CLAIMS OVER $75,000
FOR MONTH ENDING 2/28/2018

CLAIM NUMBER	LOSS DATE	DISTRICT	DESCRIPTION	STATUS	LOSS AMOUNT	POLICY YEAR TOTAL
POLICY YEAR	**2010-2011**					
11-0352	09/02/2010	Beaumont-Cherry Valley Water District	Diesel spill near Well 21	Closed	160,682	
13-0308	05/31/2010	Calleguas Municipal Water District	B&M Well 14	Closed	171,458	
10-1581	04/12/2010	Friant Power Authority	Lightening strike hit KV line and shorted out circuit breaker starting fire that burned for 45 minutes.	Closed	1,244,845	
11-0409	12/21/2010	Mammoth Community Water District	Quonset hut #1 collapsed	Closed	109,349	
11-0413	12/16/2010	Serrano Water District	PLD failed causing overflow in filtration tank into gallery	Closed	75,959	
			POLICY YEAR 2010-2011		**1,762,294**	**2,494,649**
POLICY YEAR	**2011-2012**					
12-0495	09/10/2011	Arvin-Edison Water Storage District	Lightning strike damage 3 - 5,500 HP motors @ Forest Frick Pump Station	Closed	616,557	
14-0508	12/27/2011	Bard Water District	Employee dishonesty	Closed	100,000	
12-0101	08/12/2011	Fresno Irrigation District	Kitchen fire @ 9451 E. Olive	Closed	139,653	
12-0049	07/13/2011	Helix Water District	Explosion in Ozone Destruct Unit #2	Closed	224,117	
12-0190	09/10/2011	Kern County Water Agency	Switch gear @ 2B & 4B melted	Closed	164,802	
12-0112	07/07/2011	Lower Tule River Irrigation District	Bearing damage @ LakeSuccess Turbine	Closed	293,739	
12-0171	09/07/2011	Mission Springs Water District	Sprinkler system went off sending 3" of water into building	Closed	214,319	
			POLICY YEAR 2011-2012		**1,753,186**	**2,508,715**
POLICY YEAR	**2012-2013**					
12-0769	05/07/2012	Banta Carbona Irrigation District	B&M - Pumping Station #1	Closed	207,856	
13-0393	12/11/2012	Del Puerto Water District	Unknowns stole 200K generator/utility trailer	Closed	88,000	
12-0681	05/01/2012	Palmdale Water District	Hydro-electric generator burned.	Closed	292,341	
13-0336	12/02/2012	South Feather Water and Power Agency	Tree fell into shop building	Closed	127,212	
			POLICY YEAR 2012-2013		**715,409**	**1,273,296**

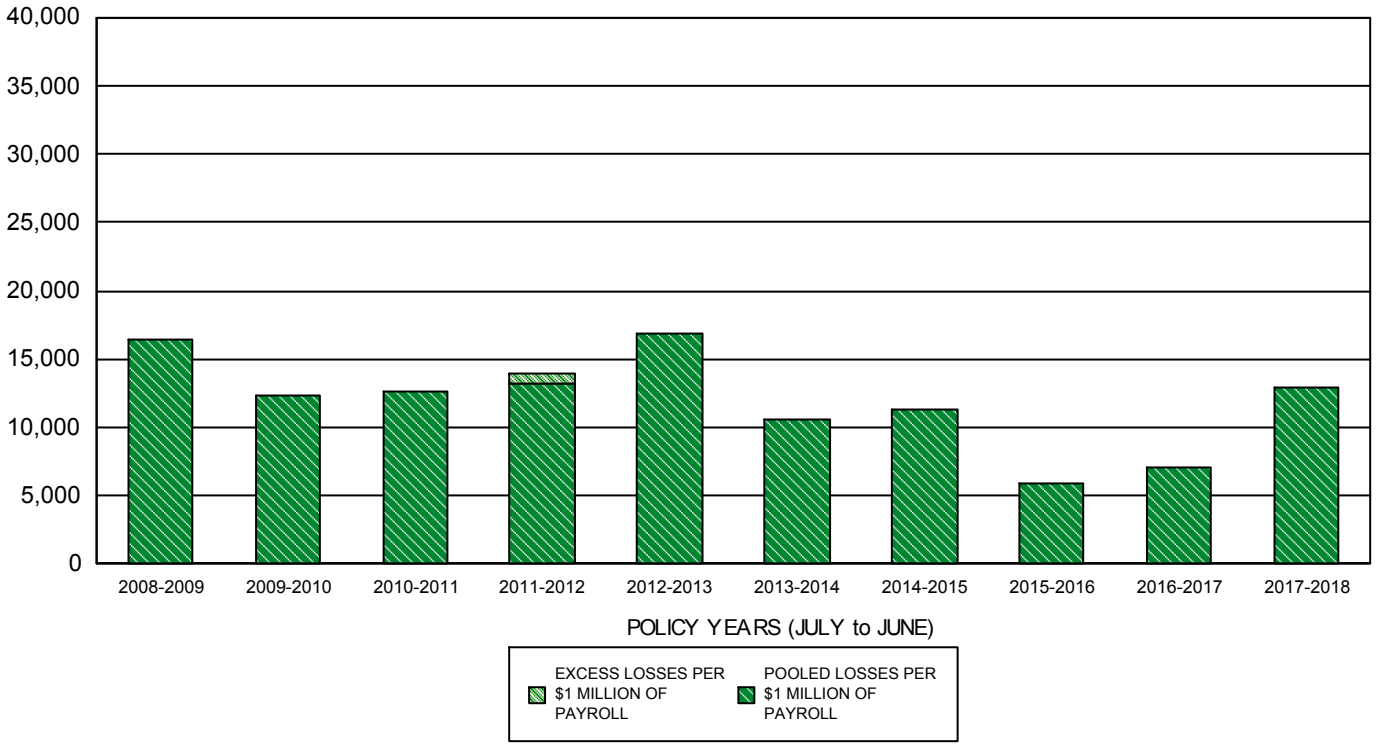
ACWA JPIA - PROPERTY PROGRAM
SIGNIFICANT LARGE CLAIMS OVER $75,000
FOR MONTH ENDING 2/28/2018

CLAIM NUMBER	LOSS DATE	DISTRICT	DESCRIPTION	STATUS	LOSS AMOUNT	POLICY YEAR TOTAL
POLICY YEAR		**2013-2014**				
13-0658	04/25/2013	Bella Vista Water District	1,000 HP pump/motor @ Wintu failed	Closed	149,736	
14-0396	01/22/2014	Coastside County Water District	Fire in District's server room	Closed	277,915	
13-0644	04/20/2013	Fresno Metropolitan Flood Control District	Theft of copper wire	Closed	77,400	
14-0548	03/24/2014	Oakdale Irrigation District	Excavator caught fire & burn	Closed	162,003	
14-0320	12/03/2013	Twentynine Palms Water District	Generator at flouride removal treatment plant failed.	Closed	119,755	
			POLICY YEAR 2013-2014		**786,808**	**1,450,265**
POLICY YEAR		**2014-2015**				
15-0514	11/30/2014	Serrano Water District	Line break/surge caused damage @ Smith Reservoir	Open	107,727	
15-0454	02/06/2015	Wheeler Crest Community Services District	Wildfire burned District's building & contents @ Rimrock Regulation Station	Closed	80,123	
			POLICY YEAR 2014-2015		**187,851**	**809,445**
POLICY YEAR		**2015-2016**				
16-0100	07/09/2015	Orange County Water District	Vandalism/fire damaged HDPE pipe @ Santiago Basin	Closed	416,000	
16-0230	10/06/2015	Thermalito Water & Sewer District	Fire @ District office	Closed	152,104	
			POLICY YEAR 2015-2016		**568,104**	**1,269,376**

ACWA JPIA - PROPERTY PROGRAM
SIGNIFICANT LARGE CLAIMS OVER $75,000
FOR MONTH ENDING 2/28/2018

CLAIM NUMBER	LOSS DATE	DISTRICT	DESCRIPTION	STATUS	LOSS AMOUNT	POLICY YEAR TOTAL
POLICY YEAR		**2016-2017**				
17-0499	02/09/2017	Clearlake Oaks County Water District	District reports flood damage to lift stations due to Clearlake reaching flood stages during storm.	Closed	768,770	
16-0591	04/07/2016	Placer County Water Agency	During a planned outage, water backed up into electrical area of Foothill Treatment Plant because a valve wasn't opened.	Closed	678,179	
16-0693	04/17/2016	Reclamation District #2068	Circuit breaker failure resulted in control cabinet fire	Closed	101,198	
17-0732	03/28/2017	South Coast Water District	District employee misappropriated cash received from District's tennis center.	Open	104,000	
17-0474	02/10/2017	South Feather Water and Power Agency	Debris from Oroville's damaged spillway caused water to back up and flood the Kelly Ridge Powerhouse.	Open	3,300,000	
17-0583	03/07/2017	Water Replenishment District of Southern California	Field Office & Storage Annex Burglarized and vandalized.	Open	222,500	
17-0505	02/17/2017	West Valley Water District	Recent storms washed out box culvert at tank site 2-2/2-3.	Open	95,000	
			POLICY YEAR 2016-2017		**5,269,646**	**5,995,048**
POLICY YEAR		**2017-2018**				
18-0131	08/14/2017	Arvin-Edison Water Storage District	Damage to 5500 HP motor @ Forest Frick Plant	Open	107,276	
18-0348	12/10/2017	Montecito Water District	Thomas Fire damaged/burned District property @ Juncal Dam Site	Open	810,000	
18-0222	10/09/2017	Redwood Valley County Water District	Wildfire damaged District's Tomki Booster Pump Station	Open	328,000	
18-0220	07/06/2017	Scotts Valley Water District	Water main break damaged booster pump station & booster pump equipment	Open	102,500	
17-0730	05/01/2017	Tahoe City Public Utility District	Various items damaged due to heavy snow storm	Open	104,999	
			POLICY YEAR 2017-2018		**1,452,775**	**2,348,326**
				GRAND TOTAL	**25,390,853**	

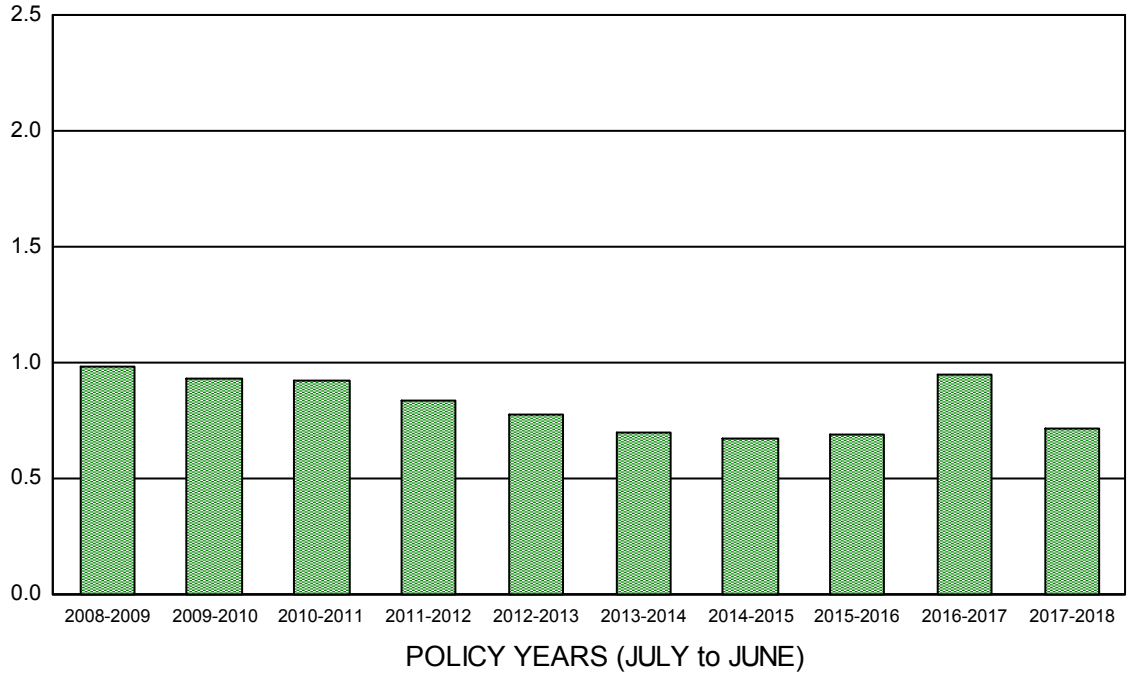
ACWA JPIA - WORKERS' COMPENSATION PROGRAM
REPORTED LOSSES PER $1 MILLION OF PAYROLL REPORT
FOR MONTH ENDING 2/28/2018



PROGRAM YEAR (7/1)	# OF MEMBERS	SELF INSURED RETENTION	POOLED LOSSES	EXCESS LOSSES	TOTAL LOSSES	ACTUAL PAYROLL	EXCESS LOSSES PER $1 MILLION OF PAYROLL	TOTAL LOSSES PER $1 MILLION OF PAYROLL
2003-2004	148	2,000,000	3,718,466	0	3,718,466	293,598,986	0	12,665
2004-2005	152	2,000,000	3,231,684	0	3,231,684	313,397,689	0	10,312
2005-2006	152	2,000,000	2,854,700	0	2,854,700	323,787,008	0	8,817
2006-2007	152	2,000,000	2,088,292	0	2,088,292	334,631,058	0	6,241
2007-2008	152	2,000,000	4,623,316	0	4,623,316	383,018,244	0	12,071
2008-2009	151	2,000,000	6,241,683	0	6,241,683	378,180,537	0	16,505
2009-2010	154	2,000,000	4,772,553	0	4,772,553	387,355,399	0	12,321
2010-2011	161	2,000,000	5,009,318	0	5,009,318	397,385,704	0	12,606
2011-2012	165	2,000,000	5,369,241	306,255	5,675,496	407,655,190	751	13,922
2012-2013	171	2,000,000	7,251,027	0	7,251,027	428,168,461	0	16,935
2013-2014	177	2,000,000	4,740,044	0	4,740,044	445,374,309	0	10,643
2014-2015	175	2,000,000	5,131,743	0	5,131,743	453,070,613	0	11,327
2015-2016	180	2,000,000	2,824,069	0	2,824,069	471,930,942	0	5,984
2016-2017	186	2,000,000	3,561,135	0	3,561,135	503,225,727	0	7,077
2017-2018	187	2,000,000	2,134,835	0	2,134,835	247,960,080	0	12,914

- Latest Policy Year's 'Losses' include partial activity.
- Latest Policy Year's 'Losses Per $1 Million of Payroll' have been annualized using 8 months data.

ACWA JPIA - WORKERS' COMPENSATION PROGRAM
CLAIMS PER $1 MILLION OF PAYROLLS REPORT
FOR MONTH ENDING 2/28/2018



PROGRAM YEAR (7/1)	NUMBER OF CLAIMS	ACTUAL PAYROLLS	INFLATION ADJUSTMENT FACTOR	INFLATION ADJUSTED PAYROLLS	NUMBER OF CLAIMS PER $1 MILLION OF INFLATION ADJUSTED PAYROLLS
2003-2004	465	293,598,986	1.344	394,534,378	1.179
2004-2005	418	313,397,689	1.312	411,269,149	1.016
2005-2006	404	323,787,008	1.274	412,527,150	0.979
2006-2007	392	334,631,058	1.224	409,551,608	0.957
2007-2008	400	383,018,244	1.191	456,004,086	0.877
2008-2009	420	378,180,537	1.131	427,582,652	0.982
2009-2010	408	387,355,399	1.131	437,956,036	0.932
2010-2011	415	397,385,704	1.131	449,296,610	0.924
2011-2012	382	407,655,190	1.122	457,249,613	0.835
2012-2013	363	428,168,461	1.090	466,723,501	0.778
2013-2014	335	445,374,309	1.071	476,894,572	0.703
2014-2015	323	453,070,613	1.051	476,089,856	0.678
2015-2016	335	471,930,942	1.027	484,758,968	0.689
2016-2017	323	503,225,727	1.014	510,270,887	0.950
2017-2018	179	247,960,080	1.000	247,960,080	0.722

- Latest Policy Year's 'Number of Claims' include partial activity.
- Latest Policy Year's 'Number of Claims Per $1 Million of Inflation Adjusted Payrolls' has been annualized using 8 months data.
- Payrolls Adjusted for Inflations - CNP's Omitted.
- Factor based on CPI for West Coast from US Dept of Labor

ACWA JPIA - WORKERS' COMPENSATION PROGRAM
SIGNIFICANT LARGE CLAIMS
WITH LOSS AMOUNTS OVER $100,000
FOR MONTH ENDING 2/28/2018

DISTRICT	CLAIM NUMBER	DESCRIPTION	STATUS	LOSS AMOUNT
POLICY YEAR 1984-1985				
Helix Water District	96108536	stained shoulder	Open	168,947.59
Valley Center Municipal Water District	96248517	slipped hurt both ankles	Closed	220,003.63
			TOTALS	**388,951.22**
POLICY YEAR 1985-1986				
Helix Water District	96108611	valley fever	Closed	260,065.14
			TOTALS	**260,065.14**
POLICY YEAR 1988-1989				
Helix Water District	96108916	herniated disc	Open	107,711.95
Western Municipal Water District	96268907	hands- applying pressure on ha	Closed	155,552.31
			TOTALS	**263,264.26**
POLICY YEAR 1989-1990				
Mission Springs Water District	96089006	r. shoulder & back-strained du	Closed	132,131.43
Western Municipal Water District	96269002	back- removing meter box.	Closed	126,817.22
Yolo County Flood Control & Water Conservation District	96279002	sharp pain in neck-ee picking	Closed	107,393.16
			TOTALS	**366,341.81**
POLICY YEAR 1990-1991				
Palo Verde Irrigation District	96349108	l. shoulder-muscle pulled	Closed	104,996.63
			TOTALS	**104,996.63**
POLICY YEAR 1991-1992				
Browns Valley Irrigation District	96029203	injury climbing on stairs	Closed	152,157.23
San Diego County Water Authority	96189201	uppr back strain	Closed	241,616.72
Yolo County Flood Control & Water Conservation District	96279206	leg, hip and foot	Open	486,333.34
			TOTALS	**880,107.29**
POLICY YEAR 1992-1993				
Butte Water District	96039301	lft thumb;amputated when his h	Closed	165,952.26
Reclamation District #108	96379301	low back strain	Closed	196,879.55
			TOTALS	**362,831.81**

ACWA JPIA - WORKERS' COMPENSATION PROGRAM
SIGNIFICANT LARGE CLAIMS
WITH LOSS AMOUNTS OVER $100,000
FOR MONTH ENDING 2/28/2018

DISTRICT	CLAIM NUMBER	DESCRIPTION	STATUS	LOSS AMOUNT
POLICY YEAR 1994-1995				
Palo Verde Irrigation District	96349505	shldr - strn,sprn,dsloc-liftin	Closed	255,098.84
Paradise Irrigation District	01-3253	bilateral upper extremities, left and right shoulder including hands, low back bilateral lower extremities caused from unknown reasons. the district first notice of this was from an attorney.	Closed	143,842.58
Walnut Valley Water District	96259503	low back/while working ee had	Closed	226,618.16
			TOTALS	**625,559.58**
POLICY YEAR 1995-1996				
Calaveras County Water District	83158	possible chemical expos	Open	216,177.09
Mission Springs Water District	09667	turning/water valve	Closed	100,646.18
Rancho California Water District	62037	lifting vault lid	Closed	128,348.57
San Diego County Water Authority	69669	pulling meter	Closed	132,128.68
Western Municipal Water District	09184	lifting a concret meter	Closed	100,576.84
			TOTALS	**677,877.36**
POLICY YEAR 1996-1997				
Oakdale Irrigation District	40940	cleaning trash fr gate	Closed	106,631.09
Paradise Irrigation District	18354	painting overhead	Open	196,569.79
Reclamation District #108	90522	boom fell	Open	683,778.02
Reclamation District #108	90525	picked up boom off co-wk	Open	114,138.28
Soquel Creek Water District	83351	using jackhammer	Open	124,649.39
Valley Center Municipal Water District	24013	open electrical panel	Open	266,601.93
Water Employee Services Authority	91769	tire blow out	Closed	131,738.51
			TOTALS	**1,624,107.01**
POLICY YEAR 1997-1998				
East Contra Costa Irrigation District	75977	twisted his right knee	Open	383,845.00
Humboldt Community Services District	38478	running wacker	Open	277,584.05
Rainbow Municipal Water District	54476	putting equipment back	Open	103,033.34
South Sutter Water District	49729	lifting spray tank	Open	240,270.76
Tahoe City Public Utility District	81104	situational stress	Closed	139,097.99
Walnut Valley Water District	75607	moving meter assembler	Open	102,183.80
Water Employee Services Authority	56277	loosening water valve	Open	139,708.22
			TOTALS	**1,385,723.16**

ACWA JPIA - WORKERS' COMPENSATION PROGRAM
SIGNIFICANT LARGE CLAIMS
WITH LOSS AMOUNTS OVER $100,000
FOR MONTH ENDING 2/28/2018

DISTRICT	CLAIM NUMBER	DESCRIPTION	STATUS	LOSS AMOUNT
POLICY YEAR 1998-1999				
Carmichael Water District	99-1569	pulled on chain on back of dumpster and right wrist popped.	Closed	106,837.37
Newhall County Water District	99-1639	alleges cumulative stress and strain of employment	Closed	146,277.45
Orange County Water District	99-1430	strained back while digging out a sprinkler.	Closed	113,924.13
San Diego County Water Authority	99-1408	strained back while opening barbed wire gate	Closed	163,550.89
South Coast Water District	99-1682	while working to repair a service break, digging to expose the water main with a hand shovel. felt a pull in his back and became increasingly more painful.	Closed	134,541.58
South Coast Water District	99-1423	stuck an underground power line while digging with a pneumatic clay spade to create a clearance around a water line.	Closed	1,623,099.76
			TOTALS	**2,288,231.18**
POLICY YEAR 1999-2000				
Merced Irrigation District	00-2265	twisted back while pushing concrete.	Open	825,731.46
Palo Verde Irrigation District	00-2205	cumulative trauma	Closed	165,800.24
Reclamation District #108	00-2543	lumbar strain caused when putting pads on crane.	Closed	161,288.46
Soquel Creek Water District	00-2373	alleged cumulative trauma	Closed	243,428.23
Trabuco Canyon Water District	00-1939	lifting a jack hammer out of a ditch, 4 1/2 feet deep, to ground level.	Closed	173,448.70
			TOTALS	**1,569,697.09**

ACWA JPIA - WORKERS' COMPENSATION PROGRAM
SIGNIFICANT LARGE CLAIMS
WITH LOSS AMOUNTS OVER $100,000
FOR MONTH ENDING 2/28/2018

DISTRICT	CLAIM NUMBER	DESCRIPTION	STATUS	LOSS AMOUNT
POLICY YEAR 2000-2001				
Consolidated Irrigation District	01-2685	motor vehicle accident	Closed	683,246.54
Fallbrook Public Utility District	01-2866	lifted oxygen tank off of mount of welding truck and felt pain in his back, right hip, and leg.	Open	115,771.80
Montecito Water District	01-3286	lumbar strain caused when moving pipes.	Closed	197,172.26
Montecito Water District	01-3443	ct	Closed	126,439.20
Otay Water District	01-2957	lumbar strain caused when responding to an alarm at the treatment plant when he stepped off the catwalk and turned towards an engine located off the catwalk.	Closed	519,410.43
Otay Water District	01-3444	hand and thumb pain caused from heavy typing and keying.	Closed	744,366.77
Otay Water District	01-3324	tingling sensation in right arm and wrist caused when operating a payment processing machine.	Closed	110,304.93
Palmdale Water District	01-2821	using district bathroom and black widow spider bit him on the left arm	Closed	1,269,807.75
Rancho California Water District	01-3309	pain in lower back and left leg caused when digging, driving, moving, that occurred over a three month period.	Closed	122,747.62
Scotts Valley Water District	01-3398	limited motion and pain to right shoulder area, the rotator cup that occurred when shoveling in the reclaim tank ditch.	Closed	142,323.45
Soquel Creek Water District	01-2811	alleged cumulative trauma	Closed	104,504.63
Tehama-Colusa Canal Authority	01-2978	pain in the groin area caused when moving hydro crane pushing block (hook) to secure it in place for transport.	Closed	120,984.21
Trabuco Canyon Water District	01-3393	neck, back, and lumbar strain that occurred when on a service call in a district owned vehicle he was rear-ended.	Closed	199,572.77
			TOTALS	**4,456,652.36**

ACWA JPIA - WORKERS' COMPENSATION PROGRAM
SIGNIFICANT LARGE CLAIMS
WITH LOSS AMOUNTS OVER $100,000
FOR MONTH ENDING 2/28/2018

DISTRICT	CLAIM NUMBER	DESCRIPTION	STATUS	LOSS AMOUNT
POLICY YEAR 2001-2002				
Amador Water Agency	02-3817	deep cut on top of left foot caused when using a gas powered weed eater to cut tall grass he hit a rock that was hidden by the tall grass. the cutting blade broke off and struck him on the top of his foot.	Closed	102,526.13
Central Basin Municipal Water District	02-3893	standing on ladder stepped down and experienced pain.	Closed	145,484.81
Coastside County Water District	02-4308	twisted left knee when shoveling rock.	Closed	143,487.41
Consolidated Irrigation District	02-4325	head, back, and ribs were injured when employee was driving a district vehicle, he was in an auto accident.	Closed	189,419.05
Desert Water Agency	02-4031	pain and numbness which began in his back right side caused when he was standing up from a stooped position he experienced the pain.	Closed	188,111.78
Elsinore Valley Municipal Water District	02-4233	while reading meters, twisted right knee	Closed	112,460.73
Humboldt Community Services District	02-3702	injury to ankles when prepping an area on the roof for painting he reached at an odd angle, became unsteady and fell. his feet became tangled in the ladder steps.	Closed	209,960.65
Municipal Water District of Orange County	02-4311	sprained right arm and side of neck caused while using the computer and the phone.	Closed	237,408.88
Orange County Water District	02-4126	superfacial lacerations to back, shoulders, neck and arms caused when closing a rolling gate.	Open	120,328.96
Quartz Hill Water District	03-5027	continuous trauma	Closed	141,706.09
Riverview Water District	02-4161	low back, right lower extremities, (leg, ankle, feet) pains that occurred during the course of his job.	Closed	175,543.47
Santa Ynez River WCD Improvement District No. 1	02-3590	lumbar, right hip, and neck area were injured when employee was preparing to install a water service and meter when another employee was spraying the area with water for dust control the employee was shutting down the hose which diverted towards claimant.	Open	531,893.96
			TOTALS	**2,298,331.92**

ACWA JPIA - WORKERS' COMPENSATION PROGRAM
SIGNIFICANT LARGE CLAIMS
WITH LOSS AMOUNTS OVER $100,000
FOR MONTH ENDING 2/28/2018

DISTRICT	CLAIM NUMBER	DESCRIPTION	STATUS	LOSS AMOUNT
POLICY YEAR 2002-2003				
East Contra Costa Irrigation District	03-4916	employee suffers pain in both knees as a result of repetitive activities.	Closed	135,230.45
Merced Irrigation District	03-4725	massive head trauma caused when changing oil filter on gradall. the hood was open. he grabbed the hood to stabilize himself and the hood closed causing him to fall.	Closed	196,509.47
Newhall County Water District	03-5131	employee strained lumbar in the course of either shoveling or pulling a hose out of mud.	Closed	354,567.49
Padre Dam Municipal Water District	03-4640	pain in right side of body, arm, leg and foot caused when shoveling dirt.	Closed	126,668.61
Rancho California Water District	03-4981	while lifting cement meter lids repeatedly, employee started to feel lower back pain.	Closed	114,188.45
Rancho California Water District	03-4792	lower back pain experienced while bending over to read meter	Closed	123,861.70
Reclamation District #108	03-5255	employee suffered shoulder strain as a result of lifting 20 lb chemical bottles.	Closed	145,923.63
San Gabriel County Water District	03-4714	tore, damaged tissue in left knee caused when shoveling and squatting to put in a water service.	Closed	117,273.30
Yolo County Flood Control & Water Conservation District	03-5191	employee suffered a lumbar strain after slipping while stepping from board walk to cement. employee did not fall but twisted his back.	Closed	117,782.53
			TOTALS	**1,432,005.63**

ACWA JPIA - WORKERS' COMPENSATION PROGRAM
SIGNIFICANT LARGE CLAIMS
WITH LOSS AMOUNTS OVER $100,000
FOR MONTH ENDING 2/28/2018

DISTRICT	CLAIM NUMBER	DESCRIPTION	STATUS	LOSS AMOUNT
POLICY YEAR 2003-2004				
Calaveras County Water District	04-5911	employee injured his right wrist and elbow when he slipped and fell on some ice while performing an inspection.	Closed	165,882.79
Calleguas Municipal Water District	04-5357	employee suffers from whiplash as a result of being rear-ended while stopped at a traffic light in a district vehicle.	Closed	111,817.17
Helix Water District	04-5715	employee has swollen knees due to repeated climbing lake terrain	Open	311,033.95
Orange County Water District	04-5761	strain to neck and middle back when employee got off dozer	Open	140,177.07
Otay Water District	04-5559	employee experienced pain and swelling in both hands and her fingers as a result of keyboarding.	Closed	103,789.98
Reclamation District #108	04-6231	burns to hands, arms face while trying to start pump	Open	176,176.25
San Diego County Water Authority	04-5924	injured left hand and fingers - while inspecting area employee made contact with blade of rotary fan. the fan guard had been removed.	Closed	120,189.05
San Juan Water District	04-5473	employee felt sharp pain in lower back when stepping on a shovel and rocking the handle side to side. employee also heard a pop.	Open	257,596.01
Santa Clarita Valley Water Agency	04-6041	employee injured his right knee when he stepped over a drain pipe and slipped.	Closed	155,061.86
Stockton-East Water District	04-5977	landed on buttocks when slipped and fell while pulling on a rope	Open	156,249.55
			TOTALS	**1,697,973.68**
POLICY YEAR 2004-2005				
Consolidated Irrigation District	05-6396	shoulder and back pain after travel to read wells	Closed	117,152.61
Elsinore Valley Municipal Water District	05-7207	asthma from cloud of sand blasting materials	Closed	401,551.64
Helix Water District	05-7142	right knee strain while standing on a ladder	Closed	146,249.41
Palmdale Water District	05-7240	left ankle, left shoulder, left arm, right knee and back strain after hose struck employee	Closed	166,982.65
Quartz Hill Water District	05-6897	dirt/rock in both ears while bending over pipe when loose piece of dirt fell on his head	Closed	358,412.64
San Luis & Delta-Mendota Water Authority	05-6707	strain to left shoulder, neck and spine after pouring concrete	Open	145,713.28
Sweetwater Authority	05-7255	right knee strain from climbing down ladder	Closed	144,675.20
Yolo County Flood Control & Water Conservation District	06-7427	strained middle and lower back when fell walking downhill.	Closed	345,749.00
			TOTALS	**1,826,486.43**

ACWA JPIA - WORKERS' COMPENSATION PROGRAM
SIGNIFICANT LARGE CLAIMS
WITH LOSS AMOUNTS OVER $100,000
FOR MONTH ENDING 2/28/2018

DISTRICT	CLAIM NUMBER	DESCRIPTION	STATUS	LOSS AMOUNT
POLICY YEAR 2005-2006				
Orange County Water District	06-8222	death, possibly due to heart attack while sitting in truck.	Closed	191,450.65
Orange County Water District	07-8605	back injury from repetitive sitting on bulldozer and heavy equipment	Closed	320,852.26
South Sutter Water District	06-7447	back strain & spasms from using weed eater	Open	329,400.90
Tahoe City Public Utility District	07-8553	strained lower back and tailbone from prolonged sitting at computer.	Open	259,023.62
Valley County Water District	06-7635	strained thoracic and lumbar back regions while painting office walls.	Open	345,427.31
			TOTALS	**1,446,154.74**
POLICY YEAR 2006-2007				
Walnut Valley Water District	09-0210	strained wrist performing job duties.	Closed	147,833.59
Western Municipal Water District	07-8338	electrical shock while operating backhoe when struck 12kv underground electric cable.	Closed	132,512.49
			TOTALS	**280,346.08**
POLICY YEAR 2007-2008				
Clear Creek Community Services District	08-9328	strained right shoulder moving broken concrete pieces by hand.	Closed	259,507.21
El Dorado Irrigation District	08-0028	strained neck when climbing a ladder to exit vault.	Open	550,938.63
Mammoth Community Water District	08-9423	abrasions on right hip and lower back when hit with backhoe.	Open	254,119.24
Merced Irrigation District	08-9395	strained lower back when stepped in sewer cleanout that was uncovered.	Open	153,071.24
Merced Irrigation District	08-9761	strained lower middle back while moving kelly bar with anchors and anchor rod attached.	Closed	215,266.34
Rancho California Water District	08-9830	strained lower back when bent down to pick up meter box lid.	Open	571,899.23
Sweetwater Authority	08-9373	strained lower back while mixing cement in wheelbarrow.	Closed	159,006.80
Western Municipal Water District	09-0600	contracted valley fever while performing normal duties.	Open	520,132.64
Yolo County Flood Control & Water Conservation District	08-9474	broke right leg above ankle when fell off ladder while painting.	Open	449,557.27
			TOTALS	**3,133,498.60**

ACWA JPIA - WORKERS' COMPENSATION PROGRAM
SIGNIFICANT LARGE CLAIMS
WITH LOSS AMOUNTS OVER $100,000
FOR MONTH ENDING 2/28/2018

DISTRICT	CLAIM NUMBER	DESCRIPTION	STATUS	LOSS AMOUNT
POLICY YEAR 2008-2009				
Consolidated Irrigation District	09-0906	left ankle and bilaterial legs when boot got tangled on mower door while trying to get off mower.	Open	192,696.86
Consolidated Irrigation District	09-0674	strained neck and right shoulder when grader stopped suddenly after running over stump.	Closed	390,133.41
Crescenta Valley Water District	09-0782	strained lower back and ankle when lost balance and fell while inspecting work at reservoir.	Closed	193,800.33
Crescenta Valley Water District	09-0606	strained lower back and right sciatica while shoveling.	Open	226,541.23
East Contra Costa Irrigation District	09-0819	strained right bicep while opening inline valve.	Closed	103,078.39
El Dorado Irrigation District	09-0159	strained right knee, cut right elbow when fell when climbing onto backhoe trailer when missed handle.	Open	103,485.02
Elsinore Valley Municipal Water District	09-0877	strained bilateral arms, elbow and wrists from doing repetitive computer and lab work.	Open	916,696.80
Laguna Beach County Water District	09-0655	legs, neck and back when fell 20 ft off fence when bricks gave way, landing on hood of truck, while climbing over dist fence to enter parking lot because driver forgot remote for gate.	Closed	330,683.10
Merced Irrigation District	09-0673	strained right shoulder while pulling boards out of the weirs to send water downstream.	Open	591,032.99
Mesa Water District	09-0324	strained lower back and right shin when he stepped on a curb and fell while digging a hole.	Open	592,154.51
Patterson Irrigation District	10-1016	injured right hip and back, cause unknown.	Open	177,177.93
Ramona Municipal Water District	09-0822	strained left shoulder and neck while tying backhoe to trailer when binder came loose jerking the arm back.	Closed	150,974.81
Western Municipal Water District	09-0582	back and neck injuries when veh hydroplaned, he lost control and struck ov.	Open	242,952.56
Yolo County Flood Control & Water Conservation District	09-0577	strained right clavicle and right shoulder while pushing up on trip switch to open dam gate.	Open	118,858.37
			TOTALS	**4,330,266.31**

ACWA JPIA - WORKERS' COMPENSATION PROGRAM
SIGNIFICANT LARGE CLAIMS
WITH LOSS AMOUNTS OVER $100,000
FOR MONTH ENDING 2/28/2018

DISTRICT	CLAIM NUMBER	DESCRIPTION	STATUS	LOSS AMOUNT
POLICY YEAR 2009-2010				
Antelope Valley-East Kern Water Agency	10-1719	strained left knee while walking on gravel.	Closed	259,838.03
Bella Vista Water District	10-1142	strained left knee while stepping off step.	Closed	166,626.17
Crescenta Valley Water District	10-1379	bruised left ribcage, hip and pelvis when slipped while descending ladder after filling vactor truck with diesel.	Closed	296,245.64
East Contra Costa Irrigation District	10-1730	injured rt elbow, left hip, back, shoulder and had difficulty breathing when fell while walking down stairs carrying a moss hook.	Closed	194,930.19
Elsinore Valley Municipal Water District	10-1407	strained neck and shoulder when backing dist truck when left rear tire left pavement and truck slide down slope then rolled.	Closed	134,328.06
Helix Water District	10-1428	strained right wrist after one week of breaking off concrete and cleaning welds.	Open	106,379.35
Helix Water District	10-1697	bilateral knees and back from repetitive walking, climbing ladders, kneeling and squatting.	Open	514,844.60
Orange County Water District	10-1396	bruised left hip and left shoulder when slipped and fell while reading water gauge in the rain.	Closed	125,404.71
San Luis Water District	10-1273	injured chest, back and right thigh when dump truck overturned because the load shifted.	Open	134,122.28
Serrano Water District	10-1349	leg burns from using a cut off saw	Closed	102,707.21
South Coast Water District	10-1723	strained right shoulder and right upper arm while cleaning sewer line.	Closed	107,942.84
South Coast Water District	10-1647	strained left shoulder from jetting with large heavy storm drain nozzle.	Closed	140,541.63
Weaverville Community Services District	10-1055	strained right shoulder while installing conduit in limited access attic.	Closed	111,229.81
Yolo County Flood Control & Water Conservation District	10-1625	strained right foot and ankle when hopped down to get out of canal.	Closed	297,035.37
			TOTALS	**2,692,175.89**

ACWA JPIA - WORKERS' COMPENSATION PROGRAM
SIGNIFICANT LARGE CLAIMS
WITH LOSS AMOUNTS OVER $100,000
FOR MONTH ENDING 2/28/2018

DISTRICT	CLAIM NUMBER	DESCRIPTION	STATUS	LOSS AMOUNT
POLICY YEAR 2010-2011				
Beaumont-Cherry Valley Water District	11-0848	struck and killed by motor vehicle while marking water line in street.	Closed	149,240.77
Cucamonga Valley Water District	11-0833	repetitive injuries to neck, back, bilateral shoulders, knees, hips, legs and waist.	Closed	131,633.15
El Dorado Irrigation District	11-0718	strained right shoulder while pulling "shoe" from manhole.	Open	226,383.65
Glenn-Colusa Irrigation District	11-0654	strained neck and back from repetitive operation of backhoe and other equipment.	Open	187,794.88
Kern County Water Agency	11-0507	injury to neck, rt upper extremity and bilateral feet, cause unknown.	Closed	323,878.52
Merced Irrigation District	11-0322	strained right knee while walking on uneven ground while performing work activity.	Closed	131,750.47
Merced Irrigation District	11-0104	left wrist and hand while spraying weeks when tripped and fell on driveway.	Open	202,413.15
Mesa Water District	11-0481	injured while replacing gate chain rollers when struck by gate.	Closed	137,405.17
Mission Springs Water District	11-0437	strained lower back moving tamper.	Open	450,601.94
Moulton Niguel Water District	11-0049	strained lower back while shoveling asphalt into truck.	Open	218,128.06
Ramona Municipal Water District	11-0638	injured left knee in 1997 when stood up after kneeling on retaining wall.	Closed	116,776.23
Reclamation District #108	11-0789	unknown	Open	163,690.00
South Feather Water and Power Agency	11-0037	ears (hearing), bilateral knees, pulmonary, cause unknown.	Closed	246,082.13
Walnut Valley Water District	11-0367	strained lower back while vacuuming a meter box.	Open	116,772.73
			TOTALS	**2,802,550.85**

ACWA JPIA - WORKERS' COMPENSATION PROGRAM
SIGNIFICANT LARGE CLAIMS
WITH LOSS AMOUNTS OVER $100,000
FOR MONTH ENDING 2/28/2018

DISTRICT	CLAIM NUMBER	DESCRIPTION	STATUS	LOSS AMOUNT
POLICY YEAR 2011-2012				
Calaveras County Water District	12-0074	injured left hand while driving forklift when forklift tipped over.	Open	2,306,255.18
Carpinteria Valley Water District	12-0488	strained bilateral hands, bilater wrists, forearm and rt shldr from repetitious job duties.	Open	156,654.65
Desert Water Agency	12-0083	sprained lower back while tightening bolts on gate valve.	Open	163,822.78
Elsinore Valley Municipal Water District	12-0055	strained lower back and bruised tailbone when fell backwards after tagging a sprinkler.	Closed	149,787.06
Georgetown Divide Public Utility District	12-0232	injured right side and back when he stepped off roof and fell 8-10 feet to ground.	Open	115,715.22
Helix Water District	12-0484	strained left knee when slipped on debris on asphalt while hooking bag to crane.	Closed	100,291.42
Mission Springs Water District	12-0122	injured rt knee when slipped while climbing out of hole.	Open	262,810.00
Moulton Niguel Water District	12-0518	injured left foot, left arm and right leg when tripped on paper roll and fell into desk then floor.	Open	106,248.27
Solano Irrigation District	12-0797	strained lower back and left hip when slipped while coming down ladder.	Open	204,838.25
Tulare Irrigation District	12-0295	injured bilateral knees and left wrist when fell while stepping off structure while measuring weir.	Open	251,158.30
Tulare Irrigation District	12-0306	strained left knee when lost balance, tripped after pulling a board out of a weir.	Open	109,772.98
			TOTALS	**3,927,354.11**

ACWA JPIA - WORKERS' COMPENSATION PROGRAM
SIGNIFICANT LARGE CLAIMS
WITH LOSS AMOUNTS OVER $100,000
FOR MONTH ENDING 2/28/2018

DISTRICT	CLAIM NUMBER	DESCRIPTION	STATUS	LOSS AMOUNT
POLICY YEAR 2012-2013				
Bard Water District	13-0125	strained lower back while picking up barricade and loading into bucket.	Open	493,267.89
Berrenda Mesa Water District	13-0509	strained left knee while unloading valve off service truck when valve slipped.	Open	384,480.00
Central Basin Municipal Water District	13-0399	concussion when leg gave way while walking out of meeting and hit head against a wall.	Closed	371,078.92
East Contra Costa Irrigation District	13-0534	strained right knee when tripped over concrete while installing a new gate.	Open	270,008.50
El Toro Water District	13-0504	depressed, stressed, and has sleep disorder, cause unknown.	Closed	108,613.61
Las Virgenes Municipal Water District	14-0117	injured multiple body parts for uncertain reasons.	Open	210,929.40
Mammoth Community Water District	14-0007	injured left hip while riding in golf cart over bumps and tree roots to an inspection site.	Closed	102,953.21
Mammoth Community Water District	13-0128	ruptured right hamstring while digging dirt with shovel.	Closed	115,218.01
Merced Irrigation District	13-0195	strained lower back while lifing 5 gallon buckets out of back of pickup.	Closed	187,205.55
Merced Irrigation District	13-0092	lacerated top of head while operating bulldozer on uneven land when hit head on top of dozer.	Open	235,705.97
Mesa Water District	14-0667	claiming ct hearing loss	Open	245,852.00
Paradise Irrigation District	13-0129	strained left shoulder from doing prep and installing asphalt	Open	131,147.79
Paradise Irrigation District	13-0306	strained back and neck while turning off main control valve.	Open	170,019.38
Patterson Irrigation District	13-0094	strained right shoulder while pulling starter cord on water pump.	Open	185,920.19
Ramona Municipal Water District	13-0629	strained knee performing normal duties.	Open	775,145.22
Stockton-East Water District	13-0454	dislocated right shoulder when slipped and fell while walking on wet concrete pads.	Closed	185,686.94
Sweetwater Authority	13-0206	strained neck, shoulders, upper extremities, elbows, wrists, hands and fingers while doing repetitive and cumulative work activities	Open	147,617.06
Vallecitos Water District	13-0319	strained lower back while carrying two 55 lb buckets of chlorine.	Open	506,748.95
Yolo County Flood Control & Water Conservation District	13-0067	strained lower back while adjusting fan belts when mount broke.	Closed	381,383.23
			TOTALS	**5,208,981.82**

ACWA JPIA - WORKERS' COMPENSATION PROGRAM
SIGNIFICANT LARGE CLAIMS
WITH LOSS AMOUNTS OVER $100,000
FOR MONTH ENDING 2/28/2018

DISTRICT	CLAIM NUMBER	DESCRIPTION	STATUS	LOSS AMOUNT
POLICY YEAR 2013-2014				
Banta Carbona Irrigation District	14-0615	strained mid back while spraying weeds from tractor when hit pothole in road.	Open	183,843.30
Beaumont-Cherry Valley Water District	14-0141	sprained knee after twisting ankle and falling on rocks.	Open	173,486.35
Crescenta Valley Water District	14-0753	strained left shoulder while driving truck involved in a motor vehicle accident	Open	121,437.36
Crescenta Valley Water District	14-0286	incurred contusions to lower back, wrists, elbows and shoulders after tripping over boulders.	Closed	166,346.88
Desert Water Agency	14-0537	injured neck and upper body while passenger in head on mva.	Open	212,641.55
El Toro Water District	14-0692	strained left shoulder when sledge hammer came in contact with manhole cover.	Open	123,686.46
Elsinore Valley Municipal Water District	14-0718	sprained left knee while walking from wet grass to mud and slid.	Open	295,586.68
Helix Water District	14-0308	experienced ct to lft neck and shldr from daily work duties.	Closed	126,535.71
Las Virgenes Municipal Water District	14-0736	ct to lft foot from water meter reading.	Open	133,861.89
Mammoth Community Water District	14-0311	strained left side of neck while lifting and lowering ice breaker into ice.	Open	273,348.64
San Luis & Delta-Mendota Water Authority	14-0360	strained back while lifting a pipe w/shovel as lever.	Open	447,914.50
San Luis Water District	14-0113	strained lower back while clearing tumbleweeds from canal.	Open	243,606.79
South Feather Water and Power Agency	14-0145	strained left shoulder while moving materials off of shelving.	Closed	146,966.75
Walnut Valley Water District	14-0519	ct to lft shldr, leg, foot, stress and sleep due to unknown.	Open	229,083.44
			TOTALS	**2,878,346.30**

ACWA JPIA - WORKERS' COMPENSATION PROGRAM
SIGNIFICANT LARGE CLAIMS
WITH LOSS AMOUNTS OVER $100,000
FOR MONTH ENDING 2/28/2018

DISTRICT	CLAIM NUMBER	DESCRIPTION	STATUS	LOSS AMOUNT
POLICY YEAR 2014-2015				
Alta Irrigation District	15-0310	injured back and body when dozer rolled over onto claimant.	Open	574,218.00
Clearlake Oaks County Water District	15-0395	injured left leg, arm, shoulder, and back while at desk and tripped and fell to floor.	Open	215,000.00
El Dorado Irrigation District	15-0670	strained lft leg and back while walking and fell in hole.	Open	154,796.05
El Toro Water District	15-0760	ct to neck, lft hand, fingers and arm from job duties.	Open	100,002.13
Glenn-Colusa Irrigation District	16-0303	exposed lungs while cleaning and picking up trash.	Closed	116,851.29
Kaweah Delta Water Conservation District	15-0722	strained lower back and legs climbing up onto dozer and fell backwards.	Open	106,531.44
Mission Springs Water District	15-0386	strained lower back and left leg exercising valve to close and valve broke.	Closed	107,554.45
Palmdale Water District	15-0268	laceration w/possible partial dislocation of right thumb while loading trucks when tonneau cover came down on hand.	Closed	206,288.85
Palmdale Water District	15-0553	strained right hip while pulling sample station can when twisted to set it down.	Open	191,020.00
Palmdale Water District	15-0282	experienceing ct to rt wrist due to typing.	Open	112,387.55
Santa Fe Irrigation District	15-0284	broke 4 ribs and bruised spleen falling back onto asphalt edge of excavation.	Open	101,866.53
Solano Irrigation District	15-0029	sprained lft knee stepping off weir structure; heard "pop".	Open	157,145.87
Sweetwater Authority	15-0112	alleges numbness in rt finger tips and pain from upper to lower shldr.	Open	163,154.81
Sweetwater Authority	15-0631	strained lft knee fighting off pit bull while trying to read meter.	Open	111,521.86
			TOTALS	**2,418,338.83**
POLICY YEAR 2015-2016				
Goleta Water District	16-0760	strained wrists and knees changing meters.	Open	121,164.96
Goleta Water District	16-0196	strained lft shldr pulling tape off box with hands.	Open	146,511.95
Helix Water District	16-0293	strained lower back getting gas can out of truck and fell back onto fin form.	Open	144,982.18
Laguna Beach County Water District	16-0207	sprained ankle and knee stepping in hole/ uneven terrain.	Open	138,526.50
Palmdale Water District	16-0749	lacerated left arm when fell on metal lifting machine.	Open	119,000.00
San Juan Water District	16-0447	strained lower back twisting to turn valve key.	Open	119,090.00
Trabuco Canyon Water District	16-0263	ct cervical radiculopathy and carpal tunnel due to unknown.	Open	143,590.00
			TOTALS	**932,865.59**

ACWA JPIA - WORKERS' COMPENSATION PROGRAM
SIGNIFICANT LARGE CLAIMS
WITH LOSS AMOUNTS OVER $100,000
FOR MONTH ENDING 2/28/2018

DISTRICT	CLAIM NUMBER	DESCRIPTION	STATUS	LOSS AMOUNT
POLICY YEAR 2016-2017				
Mammoth Community Water District	17-0654	strained right arm and right shoulder lifting a bucket of sludge up to sludge truck.	Open	121,000.00
Palmdale Water District	17-0154	strained lft knee stepping out of vehicle into hole and fell.	Open	115,583.10
Sweetwater Authority	17-0132	strained right thumb while keyboarding.	Open	136,000.00
Yuba County Water Agency	17-0674	crushed leg and ribs while mowing in skid steer and rolled down embankment.	Open	701,108.75
			TOTALS	**1,073,691.85**
POLICY YEAR 2017-2018				
Corcoran Irrigation District	18-0350	burned lower extremity cleaning up sulfuric acid and fell in hole with sulfuric acid.	Open	592,350.00
Desert Water Agency	18-0126	claimant felt pain in right arm and shoulder when he reached for a top cross bar after backfilling a leak	Open	127,298.18
Tehachapi-Cummings County Water District	18-0040	strained low back, lft leg and foot moving grating and grating slipped.	Open	125,644.60
			TOTALS	**845,292.78**
			GRAND TOTAL	**54,479,067.31**

ACWA JPIA
H.R. LaBounty Safety Awards Program
March 19, 2018

BACKGROUND
The JPIA safety awards program began in 1999 to promote safe workplace behavior and operations practices, and to reward those employees who demonstrate safe behavior or take part in proactive safety activities. The program was renamed the H.R. LaBounty Safety Awards Program in 2008, in honor of Harve LaBounty, Director of Risk Management, upon his retirement. This has been a very popular program with approximately 100 nominations received from participating members each year. The names of award recipients are announced at the spring and fall conferences and published in the *Perspective* and *Risk Control Bulletin*.

CURRENT SITUATION
Nominations for safety awards have gradually increased in number and moved away from the original intent to recognize and reward employee safety program participation. The program has been revised to refocus on employee participation in *significant* safety program activities, and to provide more clarity and consistency for members who wish to submit nominations.

The 2018-2019 ACWA JPIA H.R. LaBounty Safety Awards program description on the following pages; provides a program overview, criteria, nominations, notifications, and the selection process. The program recognizes water industry employees who implement significant safety improvement to prevent occupational injuries/illnesses. The program is open to all JPIA members who participate in the Workers' Compensation, Liability, and/or Property Programs. Winners will continue to be announced at the JPIA spring and fall conferences, with exceptional nominations that can be widely adopted by small, medium, and large members, receiving special recognition at the conferences.

In addition to the nominations for methods and equipment to reduce manual material handling exposures, nominations that recognize significant safety program improvements will be emphasized. This approach promotes results-oriented activities to ensure continuous improvement of the agency's safety program. Examples of employee nominations that are new to the program are listed, as well as clarification regarding nominations that are not appropriate to this program. A new fillable nomination form is available to ensure complete documentation is provided.

RECOMMENDATION
That the Risk Management Committee provide input to staff regarding the proposed changes to the H.R. LaBounty Safety Awards Program.

Prepared by: Carol Barake, Risk Management Program Manager Date prepared: February 27, 2018

2018-2019 ACWA JPIA H.R. LaBounty Safety Awards

Recognizing the JPIA water industry employees who implement significant safety program improvements

NOMINATION DEADLINES:

Fall Conference Awards: SEPTEMBER 30, 2018
Spring Conference Awards: MARCH 1, 2019

2018-2019 ACWA JPIA
H.R. LABOUNTY SAFETY AWARDS

Program Overview

The H.R. LaBounty Safety Awards Program recognizes ACWA JPIA water industry employees who implement significant safety improvements to prevent occupational injuries/illness. Winners will receive special recognition during the ACWA JPIA Fall and Spring Conferences held in November and May of each year. The names of all award recipients are published in the *Perspective* and *JPIA Source*. Selected award nominations will be posted on the JPIA's website.

Criteria

The program is open to all JPIA members who participate in the Workers' Compensation, Liability, and/or Property Programs. The JPIA safety award program recognizes results-oriented activities that increase employees' safety program participation, and ensure continuous improvement of the agency's safety program. Examples of employee nominations include but are not limited to:

- Identify new methods/equipment to reduce manual material handling exposures, especially methods based on eliminating or reducing the hazard.
- Conduct proactive ergonomic evaluations after completion of The Back School CEAS program.
- Participate in an annual review of the Injury and Illness Prevention Program, including a recommended action plan for improvements.
- Conduct a Job Safety Analysis (JSA) for a specific operation or project and deliver a safety training on the JSA to co-workers.
- Develop a Standard Operation Procedure (SOP) for a specific operation or project, and conduct a safety training for co-workers on the SOP.
- Participate in accident investigations or near-miss events that resulted in the implementation of corrective actions.
- Participate in the hazard inspection program using a customized inspection form and document corrective action for their work area.
- Develop/update a hazard inspection program for job sites in the field.
- Participate in the annual review of confined space entry permits, resulting in corrective actions to improve the program.
- Identify procedures to eliminate the need to enter a confined space.
- Participate in the review of a project-specific Contractor Safety Program.

Nominations *not* appropriate for this program:

- Achieving injury/illness rate reduction or "zero" injuries. JPIA follows best practices and does not provide incentives for programs that may discourage workers from reporting occupational injuries.
- Activities that are not results-oriented, i.e. following basic safety rules and policies.
- Nominations related to "conditions of employment", e.g. wearing or providing required PPE, or providing Safety Data Sheets.
- Nominations not directly related to the employee safety program and safety improvements in the agency operations or equipment, e.g. administrative procedures to track district property.
- Nominations that may create new safety hazards for other employees or the public.
- Equipment modifications performed without manufacturer approval, and that affect the warranty.
- Equipment fabricated in-house where a readily available commercial product that meets regulatory requirements is available, e.g. eyewash stations.
- Nominations for written safety programs, policies, and procedures to meet basic regulatory requirements, e.g. IIPP. Employee participation in an annual review of the required written program that results in corrective actions will be accepted.

2018-2019 ACWA JPIA
H.R. LABOUNTY SAFETY AWARDS

Nominations

All nominations must be received by the following deadlines:

- Fall Conference—September 30, 2018
- Spring Conference—March 1, 2019

- Nominations may be for an individual employee, a work group, safety committee members, or for an agency-wide effort.
- Each nomination must include the nomination form available on the JPIA's website, supporting documentation, and digital photos.
- Nominations with insufficient documentation will be returned with a request for the necessary information. The revised packet must be re-submitted before the deadline to be considered. Revised packets received after the deadline will be included in the next round of awards, which occur every six months.

Notifications

- A confirmation email will be sent within (5) business days of your submission.
- A second email will be sent indicating whether the nomination meets the criteria, and contains complete documentation.

Selection Process

JPIA Risk Management will review all completed nomination forms and the supporting documentation received by the deadline. Nominations will be evaluated based on Best Practices scoring criteria. The Chief Executive Officer may approve monetary awards.

Judging Criteria

The criteria for the awards are developed and reviewed regularly by JPIA Risk Management and the JPIA Risk Management Committee. JPIA anticipates that additional criteria will be added and updated in future years.

Contact Carol Barake at cbarake@acwajpia.com or Terry Lofing at tlofing@acwajpia.com for questions or additional information.

H.R. LaBounty Safety Awards Nomination Form

Nomination Deadlines:

Fall Conference Awards: September 30, 2018
Spring Conference Awards: March 1, 2019

Agency:

Project/Initiative Title:

Employee/Department/Committee Nominated:

Name(s):

Job Title/Department:

Nomination Summary

Write a brief summary of your project/initiative. Clearly state the problem/hazard recognized by the nominee and the specific reasons that they initiated corrective action.

Describe the specific actions taken to resolve the problem(s) or challenge(s). Share the best practices that made this initiative successful for the agency and its impact.

State whether the hazard was reduced with engineering controls, introduced a new administrative or work procedure, or relied on personal protective equipment to solve the problem.

Describe any extraordinary circumstances that made this nominee's safety accomplishments significant. Describe whether the nominee influenced safety in the workplace, encouraged employee participation in safety efforts, obtained organizational "buy in" to implement the solution.

Describe whether the project/initiative addressed a hazard or exposure included in the JPIA Commitment to Excellence Program.

☐Office/Field Ergonomics

☐Vehicle Operations

☐Slip/trip/falls – falls from heights

☐Other:

List and attach any supporting materials that you feel are important for the reviewers to gain a complete picture of the nomination. Digital photos, supporting documentation, sample forms, etc.

Nominated by:

Signature:

Date:

(Type Name)

General Manager:

Date:

(Type Name)

Please email this form with supporting documents and digital photos to tlofing@acwajpia.com.

ACWA JPIA
JPIA Source – Risk Management Quarterly Bulletin
March 19, 2018

BACKGROUND
The JPIA *Risk Control Bulletin* has been produced monthly by Risk Management staff since 1997. It was developed to communicate occupational health and safety information and tips for use at district safety meetings.

CURRENT SITUATION
Access to occupational health and safety resources has expanded exponentially over the past twenty years. These resources are readily available in many different formats on government agency websites such as OSHA and Cal/OSHA, as well as subscription publications such as the *Cal OSHA Reporter* and the *National Safety Council* newsletters. A new quarterly publication that frames the information specifically for water agencies and broadens the scope to include risk management best practices for liability and property risks, will fill a gap that is not addressed by other publications. The new publication has been named ***JPIA Source***, and will be published in spring (March), summer (June), fall (Sept.) and winter (December). JPIA Risk Management staff looks forward to member input on the new format, and their suggestions for future articles.

RECOMMENDATION
None, informational only.

Prepared by: Carol Barake, Risk Management Program Manager Date prepared: February 27, 2018

JPIA Source

Spring 2018 Volume 1 Issue 1

ACWA JPIA Risk Management for the Water Industry

Homeless Encampments

Clean-Up Operations: In-house or Contract Clean Up Service

Protecting Staff from Exposure to Bloodborne Pathogens and Hepatitis A

Reducing Liability Exposure: Removal, Storage and Destruction of Personal Property

ACWA JPIA
YOUR BEST PROTECTION

ACWA JPIA
Risk Management Training Update
Course Revisions and Risk Management Regional Training Calendar
March 19, 2018

BACKGROUND
The JPIA Risk Management Advisors deliver high quality, instructor led trainings to our members to reinforce best practices and reduce losses. The department typically delivers 275 classes each year, with over 4,000 participants. The trainings focus on the Defensive Driver training and Ergonomics training requirements, mandated by the JPIA Executive Committee for all members. Risk Advisors also deliver occupational health and safety topics relevant to the water industry construction and maintenance activities such as Confined Space and Trenching and Excavation. Safety management program courses are integrated into the Professional Development Program, and are also delivered by the Risk Management team.

CURRENT SITUATION
Vehicle operations and ergonomic/fall exposures remain our most significant loss areas, with frequent requests for on-site training from members. Risk Management staff has begun a comprehensive review of the claims experience in these areas to ensure that our course content reflects the best practices and controls that are most relevant. This review has led to the development of new training modules for these courses, which will increase our effectiveness. The look of the presentations is also undergoing changes, reflecting the vehicles and worksite conditions seen in the water industry. The new presentations will be peer reviewed in the April Risk Management staff meeting, and will be ready for delivery shortly afterward.

The Risk Management Regional Training Calendar for 2018-2019 has been provided to members to increase the opportunities to complete several courses for the PDP Operations certificate in one location, or to complete the Cal/OSHA 10 training requirements. The Asbestos Cement Pipe courses (initial and refresher) are also included to assist members in meeting this regulatory requirement for training at several regional training events. The Regional Training Calendar will be posted to the website, and distributed to members during Risk Advisor site meetings.

RECOMMENDATION
None, informational only.

Prepared by: Carol Barake, Risk Management Program Manager Date prepared: February 27, 2018

RM Regional Training Calendar *2018/19*

Course Date	District Name/Location	Course Title	Classes
5-16-18	Yorba Linda WD, Placentia	Regional Operations—PDP	Trenching; DigAlert/One Call Law; Confined Space Entry; LOTO
5-17-18	Yorba Linda WD, Placentia	Regional Operations—PDP	Traffic Control; Silica; IIPP; Cal/OSHA Inspections; Ergonomics
5-15-18	San Benito CWD, Hollister	Regional Operations-PDP	Underground Line Locator; ACP Refresher
5-16-18	San Benito CWD, Hollister	Regional Operations-PDP	Confined Space; Traffic Control
6-19-18	Orange CWD, Fountain Valley	Cal/OSHA 10	10-Hr Construction Industry Required Course Topics (Day 1)
6-20-18	Orange CWD, Fountain Valley	Cal/OSHA 10	10-Hr Construction Industry Required Course Topics (Day 2)
7-17-18	JPIA, Roseville	Regional Operations-PDP	Defensive Driver; Traffic Control; IIPP; Ergonomics
7-18-18	JPIA, Roseville	Regional Operations-PDP	ACP Initial & Refresher; Silica; Hazard Communication; Heat Stress
9-26-18	San Diego Training Conference	Regional Operations-PDP	Defensive Driver; Traffic Control; IIPP; Ergonomics; Accident Investigation; Hazard ID
9-27-18	San Diego Training Conference	Regional Operations-PDP	Trenching & Excavation; Confined Space; Cal/OSHA Inspections; Silica; Heat Stress; Hazard Communication
10-3-18	Bella Vista WD, Redding	Regional Operations-PDP	ACP Initial & Refresher
10-4-18	Rio Alto WD, Redding	Regional Operations-PDP	Traffic Control; Silica; TBD
10-24-18	San Luis & Delta Mendota, Los Banos	Regional Operations-PDP	Trenching/Shoring; Confined Space; Drug/Alcohol RS
10-25-18	San Luis & Delta Mendota, Los Banos	Regional Operations-PDP	Defensive Driver; IIPP; Silica
11-28-18	Oakdale ID, Oakdale	Regional Operations-PDP	ACP Initial; Underground Line Locator
11-29-18	Oakdale ID, Oakdale	Regional Operations-PDP	ACP Refresher; Silica
2-1-19	JPIA, Roseville	Regional Operations-PDP	TBD

ACWA JPIA
New Staff Position in Southern California
March 19, 2018

BACKGROUND
Risk Management staff and resources are continuing to experience heavy demands as the JPIA membership grows, and the members express interest in updated and enhanced services.

CURRENT SITUATION
The Executive Committee approved the recommendation of the Personnel Committee for a new Senior Risk Management Advisor position. The concentration of larger districts in Southern California, especially in Orange and San Diego Counties, has led to increased demands and the need for additional staff. Recruitment efforts are scheduled to begin in April 2018. The new position is expected to be filled this summer.

RECOMMENDATION
None, informational only.

Prepared by: Carol Barake, Risk Management Program Manager Date prepared: February 27, 2018

ACWA JPIA
Cyber Security Resources for JPIA Members
March 19, 2018

BACKGROUND
Cyber liability coverage became effective October 1, 2016 for all Liability Program members.

CURRENT SITUATION
Cyber insurance is designed to protect public entities from a variety of cyber risks associated with the use of electronic equipment in conducting its operations. Electronic equipment can mean anything from district's laptops, thumb drives, to sophisticated computer systems that operate pumps, disinfect drinking water, and other critical infrastructure operations. Cyber risks are also associated with storing data that belongs to others (such as employees or customers) on a computer network. This data often includes customer names and addresses, customers' credit card numbers, employees' birth dates and social security numbers, and other sensitive information.

The ACWA JPIA Cyber Liability Program is a commercial product, and is not part of the risk-sharing pool. This coverage protects members from a variety of exposures and coverages highlights are as follows:

- All Liability Program members have automatic coverage.
- The limit is $3 million per occurrence with an aggregate of $5 million.
- Range of Deductibles:
    - $10,000 deductible for revenues below $5 million
    - $25,000 deductible for revenues from $5 million to $25 million
    - $50,000 revenues above $25 million

Cyber Risk Management services are also provided through our insurance provider, XL Catlin. The attachments outline those services at your disposal.

RECOMMENDATION
None, informational only.

Prepared by: Karen Thesing, Director of Insurance Services Date prepared: February 26, 2018

RISK MITIGATION SERVICE OFFERING

SERVICE OFFERINGS:

As a benefit to being an XL Catlin Policyholder, you have complimentary access to one of the services listed on page 2 and 3 of this endorsement. This service may be utilized once during either this policy period or upon a subsequent renewal of this policy. To get started, please contact:

Mike Buratowski
Phone: 240-650-2040
Email:
Michael.buratowski@fidelissecurity.com
http://www.fidelissecurity.com/services/breach-

or

Charlie Groves
Charles R. Groves
Charlie.Groves@CrowdStrike.com
M: +1.303.887.0506

CrowdStrike Services for XL Catlin

Offering	Overview	Description
Cybersecurity Maturity Snapshot	CrowdStrike consultants are internationally recognized experts in cybersecurity planning and preparedness, information security strategy, incident response and remediation, malware analysis and research, and intelligence analysis. CrowdStrike Services has worked with countless organizations and government agencies to address their security issues. **Scope of Service:** Questionnaire assessment Phone consultation (2 hours) Provision of summary report	The **CrowdStrike Cybersecurity Snapshot** is the perfect starting point to allow your organization to determine the level of preparedness and capabilities to defend against a cyber attack. After completing the CrowdStrike cybersecurity questionnaire, your organization will have direct access to an expert cybersecurity consultant to assess the results and determine a score across five key areas: **Intelligence Collection, Detection, Incident Response, Prevention, and Governance**. Based on that consultation, CrowdStrike will provide a summary report with the final scoring in each area, as well as a description of the identified areas that need improvement. As part of a separate engagement, CrowdStrike is available to conduct a more comprehensive review and help your organization address any concerns identified as part of the Cybersecurity Maturity Snapshot. All pre-breach services are tailored to the needs of your organization and provided on a flat-fee basis.

Fidelis Services for XL Catlin

Offering	Overview	Description
Incident Response Readiness Assessment (IRRA)	Our security professionals will apply their first-hand knowledge – based on thousands of hours responding to security incidents – to evaluate, assess and validate your incident response plan and your team's readiness to respond to an incident. Scope of Service: 2 hour discussion	Fidelis will evaluate, assess and validate your IR plan, escalation matrix and your team's readiness to respond to an incident. Based on the data provided by your organization and what can reasonably be covered in a two (2) hour call, we will evaluate the plan, roles and responsibilities, policy and procedures, and controls; compare with industry best practice, identify gaps in coverage; suggest areas for improvement in process, procedures and technology. Fidelis will provide a questionnaire document for your organization to review in advance of the call. Optionally, if your organization does not have a security policy or plan, Fidelis may provide a webex overview of best practice in this area.
PCI Compliance Consultation	Understand how PCI compliance affects your business operations and entire organization, why you need to secure your network as the means to compliance, and how to start down the seemingly difficult road to compliance. Scope of Service: 2 hour discussion	Fidelis PCI Qualified Security Assessors (QSA) explain how PCI applies to your business and help you lay the groundwork of a roadmap toward efficient compliance and security. They help you define your cardholder data environment and other sensitive data and provide a high-level overview of what you need to do to protect that data, be able to identify attacks, and minimize the impact and cost of an attack.

All other terms and conditions of this Policy shall remain the same.

ACW JPIA
Cyber Liability Insurance

Cyber Liability coverage protects members from a variety of exposures and coverages such as the following:

THIRD PARTY LIABILITY

- **Security Liability:** Coverage for defense costs and damages the insured is legally obligated to pay resulting from a failure of computer security, including liability caused by theft or disclosure of confidential information, unauthorized access, and unauthorized use, denial of service attack or transmission of a computer virus.
- **Privacy Liability:** Coverage for defense costs and damages suffered by others for any failure to protect personally identifiable or confidential corporate information, whether or not due to a failure of network security. Includes unintentional violations of your privacy policy and misappropriation that results in identity theft.
- **Privacy Regulatory Proceedings (sub-limited):** Coverage for defense costs for proceedings brought by a governmental agency in connection with a failure to protect private information. Insuring agreement may include (depending on insurer) coverage for fines and penalties to the extent insurable by law. Coverage for damages, i.e. amounts the insured is required by settlement to deposit into a consumer redress fund, may be covered depending on the insurer.
- **Media Liability:** Coverage for defense costs and damages suffered by others for content-based injuries such as libel, slander, defamation, copyright, title trademark infringement, or invasion of privacy with respect to creation and dissemination of your content, including advertising. (Website media content is limited to online material only).

FIRST PARTY COVERAGE

- **Privacy Event Expenses (sub-limited):** Coverage for your fees and expenses due to a potential or actual violation of a privacy regulation. Covered expenses can include computer forensics expenses, costs for a public relations firm and related advertising to restore your reputation, notification expenses and credit monitoring services.
- **Cyber Extortion:** Reimburses the insured for expenses incurred in the investigation of an intentional computer attack or threat against the insured and any extortion payments made to prevent or resolve the threat. Payments are generally subject to full discretion by insurer.
- **Network Business Interruption:** Reimburses the insured for actual lost net income and extra expense incurred when the insured's computer system is interrupted or suspended due to a failure of network security. Dependent

ACW JPIA
Cyber Liability Insurance

Business Interruption is also available, but often subject to a sub-limit. Additionally, System Failure coverage is available upon request which provides limited coverage for business interruption due to an unintentional or unplanned system failure not caused by a failure of network security. In addition to a dollar amount retention, a waiting period retention of between 10 to 24 hours applies.

- **Digital Asset Protection:** Reimburses the insured for costs incurred to restore or recreate intangible, non-physical assets (software or data, including electronically stored credit card numbers and customer databases) that are corrupted, destroyed or deleted due to a network security attack.

Although insurance is in place to protect the agency, the Members should take the time to fully analyze vulnerable operational areas, identify your security risks, and train all employees

ACWA JPIA
Human Resources Update
March 19, 2018

BACKGROUND
The JPIA continues to assist districts with employment-related support and training to reduce employment liability claims and encourage a positive work culture. This is accomplished through classroom training, regional Human Resource meetings, and for those in the Liability Program, direct access to JPIA staff with Human Resource expertise. (See flyer next page).

CURRENT SITUATION
Traveling over 7,000 miles last summer to conduct 12 Human Resource Group Meetings and reach over 100 different districts, JPIA's HR meetings provided knowledge and networking that was invaluable to participants. Topics such as Dealing with Change, Managing Personal and Employee Stress, Onboarding New Staff and more, were shared.

During December and January, JPIA conducted the webinar, *New Employment Laws for 2018*, on three different occasions reaching over 120 participants. February brought the morning presentation from Robert Lavigna, in both north and south, on Engaging Government Employees. Participants rated the session highly valuable and were able to walk away with ideas that could be immediately utilized to improve engagement with staff. Mr. Lavigna is the Director of the Institute for Public Employee Engagement from Wisconsin.

RECOMMENDATION
None, informational only.

ACWA JPIA
YOUR BEST PROTECTION

3 WAYS

JPIA comes to the rescue for Human Resources

Staff are retiring, new staff are hired. HR knowledge related to public entity is critical and always changing. How do agencies, especially the smaller ones, keep current?

1 Classes & Meetings

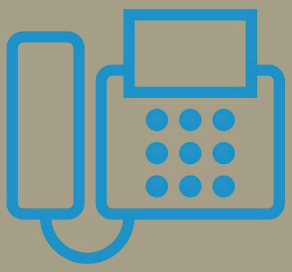
- Over 20 in-person classes
- Dozens of on-line options
- Statewide HR meetings

2 Resources

JPIA posts dozens of sample policies and forms on the website, including a complete sample job description manual. All available any time.

3 Just In Time Help

JPIA Hotline for Liability Program members fields those questions that need to be answered now. If JPIA can't help, we know who can.



ACWA JPIA
Leadership Program Update
March 19, 2018

BACKGROUND
Leadership Essentials for the Water Industry Program was rolled out in 2015, with 21 districts sending senior managers to participate in this intensive leadership training. Fall of 2015 saw 23 participants enter the inaugural program. The JPIA is focusing on the professional development of this staff level because motivated and engaged employees perform at higher levels, tend to have fewer accidents, and make fewer claims against the organization. The only effective way to achieve such positive results is through the practiced actions of effective leadership.

CURRENT SITUATION
JPIA Leadership Essentials Program graduated an additional 22 participants last fall, and has welcomed new cohorts in the north and south. For this 2017/18 session, southern California has 13 participants and northern California has 15. The Leadership Program is a deeply immersive experience that offers an opportunity for collaboration and networking, and which balances theory with back-at-work action plans.

After completion of the year-long program that included four in-person, two-day sessions and 12 webinars, the feedback from the graduates continues to be overwhelmingly positive.

Overall effectiveness rating of the program	94%
Lessons presented will help participant be a more effective leader	4.9 (of 5.0)

Due to requests from current attendees, staff is facilitating ways to keep students connected and continue to help improve their leadership skills once they complete the program. At the last spring and fall conferences, a Leadership Essential Alumni meeting was held where graduates met, networked, and discussed leadership topics and skills.

The JPIA congratulates those currently taking part in the program for dedication to their professional development, and applauds district leadership which approved staff participation. Together we will create more positive, productive staff and organizations. Further information on the Program is available on our website; click *Leadership* in the left column on the front page.

RECOMMENDATION
None, informational only.

ACWA JPIA
Training Update
March 19, 2018

Training Activity by Fiscal Year

Activity	2016/2017	2015/2016	2014/2015	2013/2014
Classes Delivered	345	335	321	321
Class Participants	5,467	5,436	5,232	5,327
Training Conferences	1	2	2	3
Training Conference Participants	62	131	88	113
Live Webinars	31*	11	21	20
Live Webinar Participants	663*	311	863	908
Recorded Webinar Viewings	591	901	601	803
Host Facilities	105	102	104	101
Target Solutions Online – Districts Active	82	135	114	--
Target Solutions - Courses Completed	15,337	14,960	11,691	11,680
PDP Completions	36	36	33	53

**October 2016 data was unavailable via WebEx, live webinar data from Nov 2016-Sept 2017*

2016/2017 Highlights:

- In February 2017, we rolled out the 2017 JPIA PDP Guide with checklist highlighting learning options including classroom, live and recorded webinar, and e-learning options for each topic.
- We have had 100 new enrollees in the 3 PDP Specialties this fiscal year; 27 in Human Resources, 33 in Operations, and 40 in the Supervisory specialties.
- New in-person classes released in 2016/2017 year: *Onboarding New Staff* and *Silica: It's Not Just Dust*.

RECOMMENDATION
None, informational only.

Prepared by: Patricia Slaven, Director of Human Resources & Administration Date prepared: February 28, 2018

JPIA MEETING & CONFERENCE CALENDAR – 2018

Meeting Dates	Board of Directors	Executive	Personnel	Finance & Audit	Programs				Risk Mgmt
					Emp. Benefits	Liability	Property	Work Comp	
Jan 18			11:00 AM Ontario						
Jan 30		1:00 PM					10:00 AM		
Mar 5		10:30 AM							
Mar 19				1:00 PM					3:00 PM
Mar 20		8:30 AM							
Apr 4					10:00 AM				
May 7	1:30 PM	10:15 AM						8:30 AM	
May 8	ACWA Conference May 8 to 11 – Sacramento								
Jun 7			11:00 AM Ontario						
Jul 9		1:00 PM			9:00 AM				
CAJPA Conference September 12 to 14 – South Lake Tahoe CA									
Sep 17				1:00 PM		3:00 PM			
Sep 18		8:30 AM							
Nov 26	1:30 PM	10:30 AM							
Nov 27	ACWA Conference November 27 to November 30 – San Diego								

	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC
JPIA Closed	1/15	19			28		4		3		12/22/23	24/25
Mgr Meetings	8	5	5	2	14	4	2	6	10	1	5	10
Staff Q&A	10	8	14	11	17	13	11	8		10	14	6
RM @ JPIA				18-19		13-14		8-9		10-11		13-14

Date Prepared: 3/1/18

Process Control System Security Guidance for the Water Sector

American Water Works Association

Dedicated to the World's Most Important Resource™

Acknowledgements

Project Advisory Committee

Don Dickinson, Phoenix Contact
Melani Hernoud, Secure Network Systems LLC
Brad Jewell, Orlando Utilities Commission
Ariz Naqvi, Alameda County Water Department
Jerry Obrist, Lincoln Water

AWWA Staff

Kevin Morley

Project Contractors

Tim Payne, EMA Inc.
Philip Gaberdiel, EMA Inc.
Bob George, EMA Inc.
Rafael Alpizar, EMA Inc.
Terry Brueck, EMA Inc.
Penny Brink, EMA Inc.

Subject Matter Expert Panel

Steve Allgeier, Environmental Protection Agency
Rebecca Bace, University of South Alabama
John Brosnan, Santa Clara Valley Water District
Vic Burchfield, Columbus Water Works
Terry Draper, HDR
Michael Firstenberg, Waterfall Security Solutions
Rod Graupmann, Pima County Regional Wastewater Reclamation Department
Steve Hansen, Las Vegas Valley Water District
Elkin Hernandez, DC Water
Darren Hollified, Jacksonville Electric Authority
James Johnson, Charlotte-Mecklenburg Utilities
Lisa Kaiser, Department of Homeland Security
Kent Knudsen, K2Share
Diana McCormick, DC Water
Eric Meyers, WaterISAC
Tony Palamara, Onondaga County Water Authority
Mike Queen, Charlotte-Mecklenburg Utilities
Robert Raffaele, American Water
Michael Richardson, Cape Fear Public Utility Authority
David Robinson, Dallas Water Utilities
Cheryl Santor, MWD of Southern California
Mary Smith, Water Research Foundation
Todd Smith, Greater Cincinnati Water Works
Shannon Spence, Arcadis
Mike Sweeney, Toho Water
Joellen Thompson, City of Grand Rapids
Jacqueline Torbert, Orange County Utilities

Project Funding

This project was funded by the American Water Works Association (AWWA), utilizing the Water Industry Technical Action Fund (WITAF), WITAF Project #503.

Revision History		
Version	**Date**	**Description**
1.0	4/4/2014	Initial Release
2.0	2/22/2017	Revised to match updated Cybersecurity Guidance tool

TABLE OF CONTENTS

1.0 Executive Overview

Within the last two decades cybersecurity threats including cyber terrorism has grown from the esoteric practice of a few specialists to a problem of general concern. National infrastructures have been found to be particularly vulnerable to such attacks. In response to this threat, a number of standards organizations have produced a wide array of standards and guidelines to assist organizations with implementing security controls to mitigate the risk from cyber-attacks. The scope of these documents is large, and the security controls in the standards often require significant planning and years of implementation.

In February 2013, the American Water Works Association (AWWA) Water Utility Council initiated a project (WITAF #503) to address the absence of practical, step-by-step guidance for protecting water sector process control systems (PCS)[1] from cyber-attacks. This action was very timely in that it coincided with the issuance of Presidential Executive Order 13636 – Improving Critical Infrastructure, on February 19, 2013, which directed the National Institute of Standards and Technology (NIST) to lead the development of a framework to reduce cyber risks to critical infrastructure. The NIST Cybersecurity Framework includes a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.

The goal of the AWWA guidance is to provide water sector utility owners/operators with a consistent and repeatable recommended course of action to reduce vulnerabilities to cyber-attacks as recommended in ANSI/AWWA G430: Security Practices for Operations and Management and EO 13636. The project is also expected to communicate a "call to action" for utility executives acknowledging the significance of securing PCS given their role in supporting water utility operations.

A panel of industry subject matter experts was consulted to identify the most pressing cybersecurity issues facing water utilities today. In response to these issues, a list of recommended cybersecurity practices was developed. This list identifies practices considered to be the most critical for managing the PCS cybersecurity risk in the water sector. Section 2.0 of this report provides a discussion of the Recommended Practices and why they are important to supporting a robust cybersecurity posture.

These recommended practices are further defined by a set of 94 cybersecurity controls that represent the more granular measures necessary to support implementation of the recommended practices. In an effort to provide water utilities with actionable tasks, a Cybersecurity Guidance Tool was developed to present these controls to users in a concise, straightforward manner.

The Cybersecurity Guidance Tool generates a prioritized list of recommended controls based on specific characteristics of the utility. The user provides information about their process control system and the manner in which it is used by choosing from a number of pre-defined use cases. For each recommended control, specific references to existing cybersecurity standards are also provided.

The tool emphasizes actionable recommendations with the highest priority assigned to those that will have the most impact in the short term. It should be noted, however, that the tool does not assess the extent to which a utility has implemented any of the recommended controls.

[1] The term process control system (PCS) is preferred over industrial control system (ICS) to avoid confusion with incident command system (ICS) common in national emergency response planning.

The AWWA Guidance and Tool represents a voluntary, sector-specific approach for adopting the NIST Cybersecurity Framework as expressed by the Water Sector Coordinating Council. This resource will be a living document, and further revisions and enhancements will be made based on user input.

The online Use Case tool was updated in 2016 based on feedback from users. The Use Case descriptions were revised for clarity. In addition, a number of additional use cases were added that address wireless communications. An additional 12 cyber controls were added. This document has been revised to match the online Use Case tool.

2.0 Recommended Cybersecurity Practices

2.1 Overview

The cybersecurity practices are a set of recommendations for improving the security posture of the process control systems (PCS) used by water and wastewater utilities. They are actionable recommendations designed to produce maximum improvement in the short term, and lay the foundations for longer term implementation of complex security programs and controls.

The list of recommended practices in Table 2-1 was compiled by a panel of key industry personnel and subject matter experts (SME) in cybersecurity and other related areas. The approach used to develop the list was to combine the operational knowledge of the SME panel with best practices and information from a number of security standards from DHS, NIST, AWWA, WaterISAC, and others. The result is a comprehensive set of recommendations that can be put into practice immediately and that will quickly yield tangible results.

2.2 Practice Categories

The practice categories were chosen by SME teams during a Definition Workshop. Each team identified important areas of security to be addressed and policies, activities, and systems that should be implemented. The recommendations from each team were then collected, integrated (to avoid duplication), and loosely organized into the ten domains of the Certified Information Systems Security Professional (CISSP) Common Book of Knowledge. Several reviews and additions followed until there was consensus that the categories and recommendations were comprehensive. The categories (like their NIST framework counterparts) are not mutually exclusive and contain significant overlap.

Governance and Risk Management

This category is concerned with the management and executive control of the security systems of the organization; it is associated with defining organizational boundaries and establishing a framework of security policies, procedures, and systems to manage the confidentiality, integrity, and availability (CIA) of the organization. One of the key components of system governance is developing and maintaining an accurate, up-to-date inventory of PCS components.

From the perspective of long-term security, this is the most important category because it creates a managed process for increasing security. It also engages the executive team by including security risks as an important part of the management of the enterprise.

Although this category of recommendations represents an essential part of an organization's security posture, the related cybersecurity controls have been assigned a slightly lower priority in order to emphasize actionable recommendations that can have significant short-term effects.

Business Continuity and Disaster Recovery

This category is concerned with ensuring that the control system continues running even when faults occur and with fast recovery after disruptions in service.

Business Continuity Planning is a structured method for an organization to prepare for and reduce the probability and impact of systems and operational failure. A key component of Business Continuity Planning is the Disaster Recovery Plan, which deals with longer disruptions from more impactful events.

Both plans require a managed process that identifies potentially disruptive events, estimates their impact, and then develops and monitors mitigation strategies.

Server and Workstation Hardening

This category is concerned with securing servers and workstations against cyber-attacks; it identifies best practices to minimize the probability

of unauthorized access to servers, and to maintain the CIA properties of the servers and the systems within them. For example, this category includes whitelisting which restricts the applications that are allowed to run in servers and workstations throughout the enterprise.

Access Control

This category is concerned with ensuring that only authorized personnel is able to access computing resources within the organization; it pertains to best practices for restricting access to computing resources and information to authorized users. For example, Single Sign On (SSN) is an access control mechanism that requires users to sign on only once; the SSN system can then use those credentials to control access to a variety of applications. However, care should be taken to ensure that different passwords are used to access PCS systems that those used to access enterprise systems.

Application Security

This category is concerned with ensuring that computer programs do *only* what they are supposed to do; for example, suppose that a module of a SCADA system is supposed to receive data from a PLC and save it. Application security contains best practices to ensure that the module is not susceptible to buffer-overflow attacks and that the data it receives does not get corrupted as it is handled by the module.

Application Security is a complex and extensive area involving the design, implementation, and testing of program modules as well as the testing and monitoring of integrated systems after implementation. Utilities should develop standard design and implementation requirements that define the testing required by software vendors and system integrators, as well as doing their own testing of the integrity of results.

Encryption

This category is concerned with ensuring that only appropriate encryption schemes are used within an organization's security systems and that the cryptography is used wherever it is needed. For example, there is general confusion of what is an appropriate encryption scheme: sometimes packing or compression algorithms are called encryption. Also, cryptographic systems must be used wherever they are needed, for example, if the data will be traveling on a public channel or via a wireless circuit, or if there is a need to provide non-repudiation of a message or a document (by using a cryptographic signature).

Weak encryption schemes are particularly dangerous because they provide little protection and create a false sense of security and complacency. Proprietary encryption schemes should be avoided since they typically have not gone through comprehensive testing and often contain flaws. Also, only encryption schemes that are referenced by appropriate standards and use keys of proper length should be considered secure.

Telecommunications, Network Security, and Architecture

This category is concerned with the security of the network infrastructure from the data connector on the wall to the enterprise switches, routers, and firewalls. This includes the physical security of the cables, the telecom closets, and the computer rooms and the protection of the data as it travels on public channels and wireless circuits. Spam filtering and website blocking are also included in this category.

The focus of this category is establishing a layered defense architecture with the PCS network at its core. It also addresses adherence to new standards for PCS network security, particularly network topology requirements within the vicinity of PCS systems and PLC controls. Another area addressed in this category is network management, including port level security.

Physical Security of PCS Equipment

Physical security is a basic requirement for all PCS Systems. Once physical access to a network device or server is achieved, compromising equipment or systems is usually a trivial matter. The recommended practices in this category focus

on preventing and restricting physical access to only authorized personnel with a need to perform some action on the hardware. The recommendations in this group are also related to monitoring, detecting, and responding to unauthorized physical access.

Service Level Agreements (SLA)

This category is concerned with the definition and management of contracts that specify services requirements to the organization. The contract manager under the direction of the executive team is responsible to define, negotiate, execute, and monitor these contracts to ensure appropriate service delivery to the organization.

An SLA is a contract which requires minimum levels of performance for services provided. For example, the Committed Information Rate (CIR) is part of a typical Wide-Area Network (WAN) services SLA and specifies the minimum bandwidth that a data circuit may have.

SLAs for PCS network systems typically focus on quality of service (QoS) rather than bandwidth. PCS systems do not require high bandwidth but cannot operate properly if the bandwidth falls below certain known thresholds.

Operations Security (OPSEC)

OPSEC is concerned with refining operational procedures and workflows to increase the security properties (CIA) of an organization. For example a utility may want to restrict what employees post on their Facebook pages about the organization's security procedures. OPSEC also includes access granting policies and procedures, security guard rotation schedules, backup recovery procedures, etc.

Education

This category is concerned with bringing security awareness to the employees, clients, and service providers of the organization.

Education involves identifying best practices and providing formal training on the security policies and procedures of the enterprise as well as security awareness and incident response. It involves test practice of the key security processes and actions to ensure quick and accurate response to security incidents within the enterprise.

Personnel Security

This category is concerned with the personal safety of employees, clients, contractors, and the general public.

Personnel security starts as part of the hiring process and ends after the employee leaves the organization. It handles periodic reaccreditation of employees and updates of the policies and procedures that govern staff. The purpose of personnel security is to ensure the safety and integrity of staff within the organization. Personnel security also applies to external contractors and service personnel, with the objective to ensure appropriate, lower privileged access to facilities.

Table 2-1
Recommended Cybersecurity Practices for the Water Sector

1. **Governance and Risk Management**
    a. Develop a formal, written Cybersecurity Policy that addresses the specific operational needs of Process Control System(s) (PCS)
    b. Establish an Enterprise Risk Management strategy that associates cybersecurity investments with enterprise business plans
    c. Perform a vulnerability assessment (CSET or physical assessment) on a regular basis.
    d. To aid in developing contingency plans, maintain current PCS asset inventory, including:
        i. Applications
        ii. Data
        iii. Servers
        iv. Workstations/HMI
        v. Field devices (e.g. PLCs)
        vi. Communications and network equipment
    e. Develop and enforce PCS hardware and software standards in order to limit number of system components
    f. Develop standard specifications language that defines PCS cybersecurity standards for inclusion in all procurement packages

2. **Business Continuity and Disaster Recovery**
    a. Develop PCS Disaster Recovery/Business Continuity Plan, including:
        i. Crisis Management Team (including at least one representative from executive management) – with authority to declare an alert or a disaster and who monitors and coordinates the necessary recovery activities
        ii. Manual overrides to allow temporary manual operations of key processes during an outage or a cyber-attack
        iii. Strategies for system redundancy (or offline standby) to ensure key system components can be restored within acceptable timeframes
    b. Ensure that corporate Incident Response Plan includes procedures and contact list for PCS
    c. Implement change management program for PLC software; maintain fully commented backups for all PLC programs and test restore process on a periodic basis
    d. Test backup and recovery plans regularly

3. **Server and Workstation Hardening**
    a. Implement whitelisting (allows only specified applications to execute on each specific computer).
    b. Maintain support contracts with HMI software vendor and implement antivirus, anti-malware, and operating system patches in accordance with vendor's direction.
    c. Implement security patch management program with periodic vulnerability scanning.
    d. Implement change management program for applications and infrastructure (routers, etc.)
    e. Harden critical servers and workstations.
    f. Remove local administrator rights, delete/disable default accounts (OS and application). Rename Administrator account
    g. Disable USB, DVD, and other external media ports
    h. Disable auto-scan of removable media

4. **Access Control**
    a. Secure PCS system access.
        i. Physical access to facilities and equipment
        ii. Application access to key software functions
        iii. External access should be controlled. Address requirements for:
            1. File exchange into or out of PCS. Include system and software updates
            2. Data exchange between PCS and others such as email (alarms), historical databases, CMMS, LIMS, etc.
            3. Establish off-line or isolated system for testing and patch management, including applications and device programs.
            4. Identify what is required for remote access. Restrict remote access to lowest level of privilege required.
        iv. Vendor, contractor system access on plant (incl. package systems). Vendor or contractor access to system should be manually initiated.
        v. Equipment (e.g. network equipment, field devices) access
    b. Secure remote access
        i. Use VPN technologies to protect information in transit.
        ii. Require multifactor authentication (e.g. tokens) for remote access to sensitive functions.
        iii. Limit access to only the minimal level required (e.g. view-only web page).
    c. Implement multi-factor authentication for all workstations.
    d. Laptops that are used to control SCADA or program field devices should be "dedicated for SCADA use only" and ports to Internet disabled. All non-essential software should be removed.

5. **Application Security**
    a. Require each PCS user to utilize unique credentials (usernames and passwords) which provide only the required level of access needed to perform their job. Establish policy for strength of password and periodic renewal. Implement automatic lock out after adjustable number of failed log-in attempts.
    b. Provide separate accounts for administrator and user functions. Do not allow users to operate with administrator rights unless actually administering the system.
    c. Provide separate credentials for PCS access from normal business access. Require different passwords between systems.
    d. Implement audit controls such as logging and monitoring of system access and modification.
    e. Aggregate system logs and conduct frequent review of network, application and systems events.

6. **Encryption**
    a. Implement device and/or storage encryption where theft or loss of a device is a possibility:
        i. Smartphones, tablets containing sensitive system information.
        ii. Laptops containing programs or other sensitive information.
        iii. Equipment (e.g. administrator passwords)
        iv. Removable media (e.g. tape, disk, USB removable storage)
    b. Implement communications encryption:
        i. Wireless communications should be encrypted where possible, regardless of type or range.
        ii. Wired communications over shared infrastructure (e.g. leased, shared) should be encrypted using VPN technologies to protect sensitive information in transit.
    c. Implement "best available" encryption
        i. Use strongest available encryption on existing equipment.
        ii. Identify encryption requirements in specifications for new equipment.
    d. Implement encryption of confidential data in on-line repositories

7. **Telecommunications, Network Security, and Architecture**
    a. Implement Layered Network Security with multiple levels of protection
        i. Utilize stateful or application layer firewalls, filtering routers, packet filtering or similar devices between networks.
        ii. Implement Intrusion Detection/Prevention Systems to identify and alarm on or block unauthorized access.
        iii. Implement security information and event management (SIEM)/anomaly detection to provide real-time monitoring of all PCS equipment.
    b. Implement network separation
        i. Implement physical (e.g. dedicated hardware) and/or logical separation (IP subnets, VLANs) to protect sensitive functions:
            1. Between PCS and other networks.
            2. Within PCS:
                a. Servers
                b. HMI
                c. Field equipment
                d. Network management
                e. 3rd party controlled equipment
            3. Over shared communications equipment or links
    c. Implement port-level security on all network devices
    d. Evaluate the risks and benefits of "pulling the plug" between PCS and the outside world. Develop an architecture that will allow critical operations to continue if isolated.
    e. Implement network management system to monitor system performance and identify potential bottlenecks.
    f. Document and periodically review PCS network architecture (including definition of PCS network boundaries)

8. **Physical Security of PCS Equipment**
    a. Control access to :
        i. Unused network ports
        ii. Removable media
        iii. Equipment cabinets and closets
        iv. Control room
        v. Facilities
        vi. Communications pathways

9. **Service Level Agreements**
    a. Identify all external dependencies and establish written Service Level Agreements and support contracts with internal and external support organizations to clearly identify expectations for response time and restoration of shared or leased network infrastructure and services, including equipment or services provided by:
        i. Equipment or service managed by IT departments
        ii. PCS vendors
        iii. Telecommunications and Internet providers
        iv. Power sources/power supply (within facilities)
        v. System vendors
        vi. System integrators
    b. Leverage procurement policies to limit number of external support organizations
    c. Establish SLA's with staff and contracted employees for responsiveness and agreement to respond in emergency conditions

10. **Operations Security (OPSEC)**
    a. Provide clear demarcation between business and PCS functions. Isolate all non-PCS functions and block access from PCS equipment to:
        i. Internet browsing
        ii. Email
        iii. Any other non-PCS access to remote systems or services
    b. Implement mobile device and portable media controls.

11. **Education**
    a. Implement a cybersecurity awareness program that includes social engineering.
    b. Provide on-going cross training for IT and PCS staff that identifies current best practices and standards for PCS cybersecurity.
    c. Provide basic network and radio communications training for PCS technicians.
    d. Participate in water sector programs that facilitate cybersecurity knowledge transfer.
    e. Identify appropriate certifications for internal and external staff. Include certification requirements in SLAs and contracts with external service providers.
    f. Provide periodic security awareness training to all employees that identifies risky behaviors and threats.
    g. Promote information sharing within your organization.

12. **Personnel Security**
    a. Implement a personnel security program for internal and contracted personnel that includes:
        i. Training
        ii. Periodic background checks
    b. Require annual and new employee signoff on PCS Cybersecurity Policy, which includes agreeing to a confidentiality statement

3.0 Cybersecurity Guidance Tool

3.1 Overview

The guidance tool is fairly simple to use, as illustrated Figure 3-1.

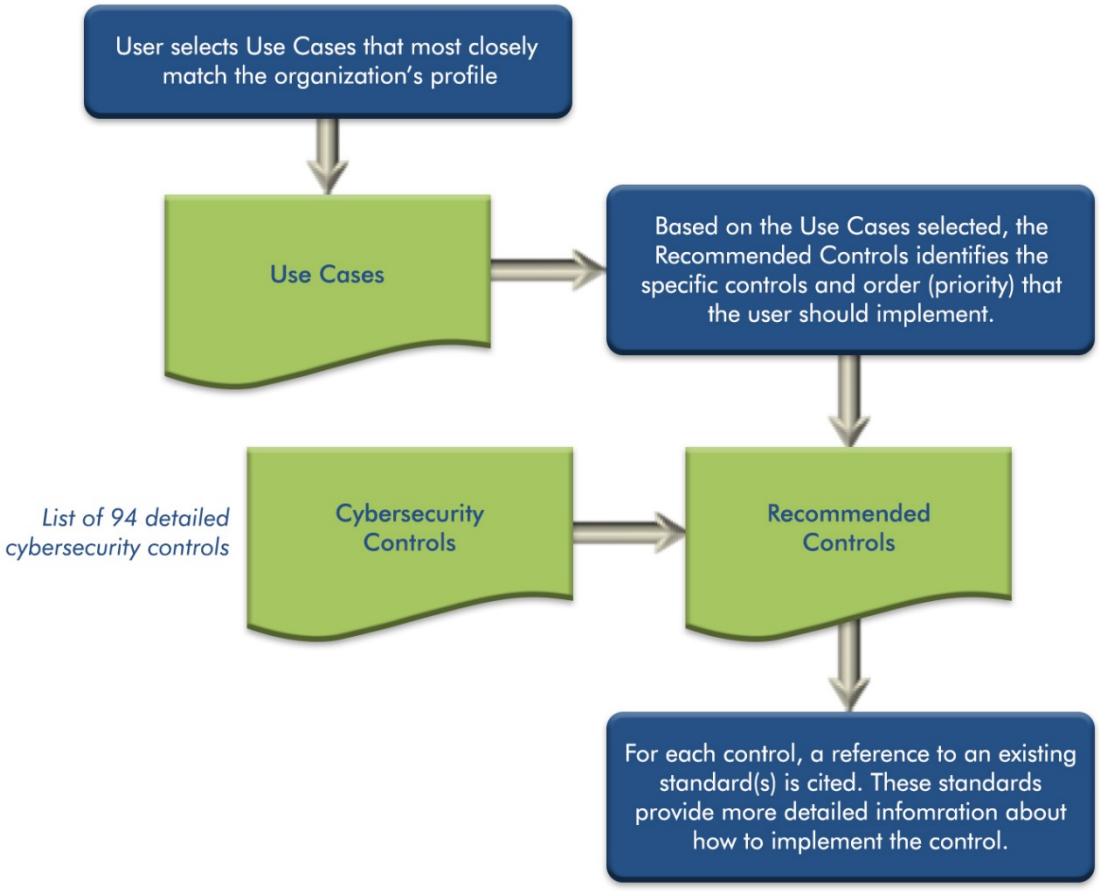


Figure 3-1
Cybersecurity Guidance Tool

The user first selects the use cases which most closely matches their utility's process control system configuration and practices. See Figure 3-2. Additional information about use cases is provided in Section 3.2. Based on the use case selections, the tool identifies the most appropriate cybersecurity controls. The recommended controls are categorized by priorities 1, 2, 3, and 4, with priority 1 being the highest. For each recommended control, a reference is provided to a set of existing cybersecurity standards.

Use Cases: (check all that apply)

CLEAR ALL

Architecture

- ☐ **AR1: Dedicated process control network.** All network and communications infrastructure is dedicated exclusively to SCADA with no equipment or communications paths shared with non-SCADA networks.
- ☐ **AR2: Shared WAN.** Network wide-area communications infrastructure is shared with non-SCADA networks.
- ☐ **AR3: Shared LAN.** Network local-area communications (within control system) is shared with non-SCADA networks.
- ☐ **AR4: Unlicensed wireless Wide-Area (site-to-site) Network.** Network wide-area communications fully or partially comprised of wireless links using unlicensed (ISM 900 MHz, 2.4 or 5 GHz) spectrum.
- ☐ **AR5: Licensed wireless Wide-Area (site-to-site) Network.** Network wide-area communications fully or partially comprised of wireless links using licensed spectrum.
- ☐ **AR6: Communications via Internet.** Network wide-area communications fully or partially comprised of links over Internet services using public address space.
- ☐ **AR7: Communications via 3rd party carrier.** Network wide-area communications fully or partially comprised of links over 3rd party carrier services (e.g. cellular, Metro-E/Ethernet/LAN).
- ☐ **AR8: Dedicated process control server virtualization.** Virtualized server infrastucture dedicated to SCADA/Process Control with no equipment shared with non-SCADA/Process Control systems.
- ☐ **AR9: Shared server virtualization.** Virtualized server infrastucture shared between SCADA/Process Control and non-SCADA/Process Control systems.
- ☐ **AR10: 802.11 wireless used in control system.** 802.11 unlicensed wireless technologies used within control system
- ☐ **AR11: Connection to non-SCADA network.** Connection to non-SCADA network through direct connection or firewall/DMZ

Network Management & System Support

- ☐ **NM1: Local network management and system support by SCADA/Process Control personnel in physical proximity of equipment.** Access to configure network equipment located in immediate vicinity of user (serial or network) by SCADA/Process Control personnel.
- ☐ **NM2: Plant network management and system support by SCADA/Process Control personnel.** Access to configure network equipment located on same facility from centralized location by SCADA/Process Control personnel.
- ☐ **NM3: Remote network management and system support by SCADA/Process Control personnel.** Access to configure network equipment located in another physical facility by SCADA/Process Control personnel.
- ☐ **NM4: Local network management and sysetm support by non-SCADA/Process Control personnel.** Access to configure network equipment located in immediate vicinity of user (serial or network) by non-SCADA/Process Control personnel.
- ☐ **NM5: Plant network management and system support by non-SCADA/Process Control personnel.** Access to configure network equipment located on same facility from centralized location by non-SCADA/Process Control personnel.
- ☐ **NM6: Remote network management and system support by non-SCADA/Process Control personnel.** Access to configure network equipment located in another physical facility by non-SCADA/Process Control personnel.

Program Access

- ☐ **PA1: Outbound messaging.** Automated, non-interactive sending of SMTP, SMS or other outbound alarms and messaging from system.
- ☐ **PA2: Outbound file transfer.** Interactive sending of files from system to other locations by user.
- ☐ **PA3: Inbound file transfer.** Interactive retrieval of files from other locations to system by user.
- ☐ **PA4: Software updates.** Automated, non-interactive retrieval of licensing, OS updates, anti-virus signatures and other system data from other locations to system.
- ☐ **PA5: Data exchange.** Automated, non-interactive exchange of data (e.g. database-to-database exchange, ntp or other external data) with systems located externally. (Implies full-time connection.)
- ☐ **PA6: Network management communications.** Automated, non-interactive exchange of network management data (e.g. syslog, SNMP traps, SNMP polling) with system(s) located external to system. (Implies full-time connection.)

PLC Programming and Maintenance

- ☐ **PLC1: Local PLC programming and maintenance.** Access to PLC programming and maintenance is local to device (serial or network).
- ☐ **PLC2: Plant PLC programming and maintenance.** Access to PLC programming and maintenance from a centralized on-site location.
- ☐ **PLC3: Remote PLC programming and maintenance.** Access to PLC programming and maintenance from an off-site location.
- ☐ **PLC4: 3rd party SCADA/Process Control presence.** SCADA/PCS equipment (e.g. PLC, RTU) owned and operated by 3rd party (e.g. business partner) located on SCADA/Process Control network with external access by 3rd party.
- ☐ **PLC5: 3rd party SCADA/Process Control package systems.** SCADA/PCS sub-systems owned and operated by 3rd parties located within plant facility with direct network connection to SCADA/Process Control system (package system) with on-site access by 3rd party.

User Access

- ☐ **UA1: Control room system access with control.** Access to system with full read-write capability from on-plant, physically secured "control room" location.
- ☐ **UA2: Plant system access with control from fixed locations.** Access to system with full read-write capability from on-plant location, not physically secured (e.g. plant floor).
- ☐ **UA3: Remote system access with control from fixed locations.** Access to system with full read-write capability from location outside "control room" environment and located outside the physical perimeter of the facility workstations or HMI.
- ☐ **UA4: Remote system access with view-only from fixed locations.** Access to system with limited read-only/view capability from location outside "control room" environment and located outside the physical perimeter of the facility workstations or HMI.
- ☐ **UA5: Remote system access with web view from fixed locations.** Access to web displays of system data with read-only/view capability from location outside "control room" environment and located outside the physical perimeter of the facility via web browser on non-dedicated computer.
- ☐ **UA6: Plant system access with control from mobile device.** Access to system with full read-write capability from on-plant location, not physically secured (e.g. plant floor) on mobile device.
- ☐ **UA7: Remote system access with control from mobile device.** Access to system with full read-write capability from location outside "control room" environment and located outside the physical perimeter of the facility on mobile device.
- ☐ **UA8: Remote system access with view-only from mobile device.** Access to system with limited read-only/view capability from location outside "control room" environment and located outside the physical perimeter of the facility on mobile device.

☐ **UA9: Remote system access with web view from mobile device.** Access to web displays of system data with read-only/view capability from location outside "control room" environment and located outside the physical perimeter of the facility via web browser on non-dedicated mobile device.

☐ **UA10: Training environment.** System training conducted on production SCADA/Process Control system by 3rd parties

☐ **UA11: Development environment by SCADA/Process Control staff.** System development conducted on production SCADA/Process Control network by SCADA/Process Control personnel.

☐ **UA12: Development environment by external staff or 3rd parties.** System development conducted on production SCADA/Process Control network by non-SCADA/Process Control personnel.

By clicking "Generate Report" you accept AWWA's **terms and conditions**.

GENERATE REPORT

Figure 3-2
Use Cases

Figure 3-3 is an example of a priority 1 list for the Local Network Management use case. A description of the cybersecurity controls and the different priorities is provided in Section 3.3. A list of referenced standards is provided in Section 3.4.

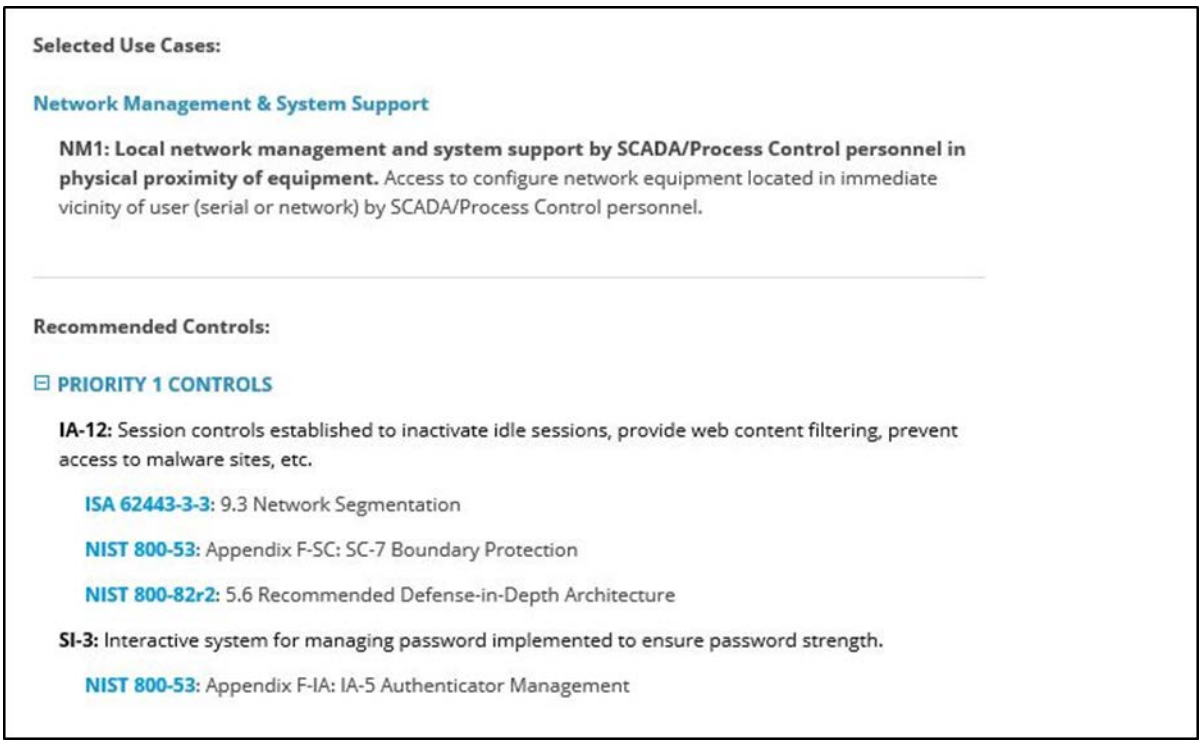


Figure 3-3
Priority 1 Controls

The Cybersecurity Guidance Tool can be used in multiple ways:

First, a user can research the security implications of implementing a procedure, changing architecture, or providing a service from the PCS network. To do this, the user selects the use case that most resembles what he wants to do and explores the results that the tool yields. The resulting controls will be grouped by priority. Priority 1 and 2 will indicate the most important controls to implement in the short term. The user can research the sources of these controls by looking at the standards-matrix which correlates the controls to the standards.

Second, a user can select all the use cases that describe his organization and by selecting the priority 1 button get a report of the top controls to implement. Users should keep in mind that a tool like this is not infallible and that a “second opinion” based on an in-depth understanding of an organization’s current security posture as well as business goals should be considered before proceeding.

Third, if an organization has already addressed the recommended priority 1 and 2 controls, they should begin to lay a security framework in order to build a comprehensive security program. The lowest priority controls (3 and 4) typically apply to the entire organization and are usually related to governance. Implementing these controls under a governance framework, like ISO 27001 or NIST 800-52, is the best way to establish a long term security program.

3.2 Use Cases

A use case is an elemental pattern of behavior as described by the user of a system; the use cases in this document are basic description of important processes within PCS from the user's perspective.

Table 3-1 provides a brief description of each use case and why it leads to different considerations for cybersecurity.

Table 3-1
Use Cases

Category/ Code	Use Case	Description	Security Considerations
Architecture			
AR1	Dedicated Process Control Network	All network and communications infrastructure is dedicated exclusively to SCADA with no equipment or communications paths shared with non-SCADA networks..	Lower network security needed here. Other issues like thumb drives and DVD usage may become a problem.
AR2	Shared WAN	Network wide-area communications infrastructure is shared with some non-SCADA networks.	High security and monitoring needed. Network topology is an issue; control of traffic into PCS network is needed.
AR3	Shared LAN	Network local-area communications (within control system) is shared with non-SCADA networks.	Very high security and monitoring needed. Authentication of users accessing PCS.
AR4	Unlicensed wireless Wide-Area (site-to-site) Network	Network wide-area communications fully or partially comprised of wireless links using unlicensed (ISM 900 MHz, 2.4 or 5 GHz) spectrum.	
AR5	Licensed wireless Wide-Area (site-to-site) Network	Network wide-area communications fully or partially comprised of wireless links using licensed spectrum.	
AR6	Communications via Internet	Network wide-area communications fully or partially comprised of links over Internet services using public address space.	
AR7	Communications via 3rd party carrier	Network wide-area communications fully or partially comprised of links over 3rd party carrier services (e.g. cellular, Metro-E/Ethernet/LAN).	
AR8	Dedicated process control server virtualization	Virtualized server infrastructure dedicated to SCADA/Process Control with no equipment shared with non-SCADA/Process Control systems.	
AR9	Shared server virtualization	Virtualized server infrastructure shared between SCADA/Process Control and non-SCADA/Process Control systems.	
AR10	802.11 Wireless used in Control System	802.11 unlicensed wireless technologies used within control system.	
AR11	Connection to non-SCADA Network	Connection to non-SCADA network through direct connection or firewall/DMZ.	
Network Management & System Support			
NM1	Local network management and system support by SCADA/Process Control personnel in physical proximity of equipment	Access to configure network infrastructure located in immediate vicinity of user (serial or network) by SCADA/Process Control personnel.	Basic access control needed. Network equipment managed from SCADA facilities only, over SCADA network infrastructure
NM2	Plant network management and system support by SCADA/Process Control personnel	Access to configure network equipment located on same facility from centralized location by SCADA/Process Control personnel.	Medium security needed.

Category/ Code	Use Case	Description	Security Considerations
NM3	Remote network management and system support by SCADA/Process Control personnel	Access to configure network infrastructure located in another physical facility by SCADA/Process Control personnel.	High security needed. High reliability on authentication of users.
NM4	Local network management and system support by non-SCADA/Process Control personnel	Access to configure network equipment located in immediate vicinity of user (serial or network) by non-SCADA/Process Control personnel.	
NM5	Plant network management and system support by non-SCADA/Process Control personnel	Access to configure network equipment located in another physical facility by non-SCADA/Process Control personnel.	
NM6	Remote network management and system support by non-SCADA/Process Control personnel	Access to configure network infrastructure located in another physical facility by non-SCADA/Process Control personnel.	
Program Access			
PA1	Outbound messaging	Automated, non-interactive sending of SMTP, SMS or other outbound alarms and messaging from system.	Routing and ACL restrictions, network topology reconsidered to ensure only outbound messages.
PA2	Outbound file transfer	Interactive sending of files from system to other locations by user.	Routing and ACL restrictions, network topology reconsidered to ensure only outbound messages.
PA3	Inbound file transfer	Interactive receiving of files from other locations to system by user.	Very high security and monitoring needed. Concern with file content. .
PA4	Software updates	Automated, non-interactive retrieval of licensing, OS updates, anti-virus signatures and other system data from other locations to system.	Very high security and monitoring needed. Concern with file content. Certificate monitoring and deep packet inspection can be used to detect issues.
PA5	Data exchange	Automated, non-interactive exchange of data (e.g. database-to-database exchange, ntp or other external data) with systems located externally. (Implies full-time connection.)	Encapsulation of data flows in a secure channel. Monitoring of payload for unusual data.
PA6	Network management communications	Automated, non-interactive exchange of network management data (e.g. syslog, SNMP traps, SNMP polling) with system(s) located external to system. (Implies full-time connection.)	Very high security and monitoring needed. SNMP security is a concern. Appropriate securing of SNMP is needed.

Category/ Code	Use Case	Description	Security Considerations
PLC Programming and Maintenance			
PLC1	Local PLC programming and maintenance	Access to PLC programming and maintenance is local to device (serial or network).	Recommended practice.
PLC2	Plant PLC programming and maintenance	Access to PLC programming and maintenance from a centralized on-site location.	Careful implementing authentication.
PLC3	Remote PLC programming and maintenance	Access to PLC programming and maintenance from an off-site location.	Not a recommended practice; two factor authentication should be in place. Dangerous!
PLC4	3rd party SCADA/Process Control presence	SCADA/PCS equipment (e.g. PLC, RTU) owned and operated by 3rd party (e.g. business partner) located on SCADA/Process Control network with external access by 3rd party.	
PLC5	3rd party SCADA/Process Control package systems	SCADA/PCS sub-systems owned and operated by 3rd parties located within plant facility with direct network connection to SCADA/Process Control system (package system) with on-site access by 3rd party.	
User Access			
UA1	Control room system access with control	Access to system with full read-write capability from on-plant, physically-secure "control room" location.	Minimal access control needed here. Other issues like thumb drives and DVD usage may become a problem.
UA2	Plant system access with control from fixed locations	Access to system with full read-write capability from on-plant location, not physically secured (e.g. plant floor).	Medium network security needed here. Other issues like thumb drives and DVD usage may become a problem.
UA3	Remote system access with control from fixed locations	Access to system with full read-write capability from location outside "control room" environment and located outside the physical perimeter of the facility workstations or HMI.	Very rigorous access control and monitoring needed to authenticate remote users. Network topology is an issue; control of traffic into PCS network is needed.
UA4	Remote system access with view-only from fixed locations	Access to system with limited read-only/view capability from location outside "control room" environment and located outside the physical perimeter of the facility workstations or HMI.	Special one way controls are needed. One way data flow can be done by ACLs or specialized equipment.
UA5	Remote system access with web view from fixed locations	Access to web displays of system data with read-only/view capability from location outside "control room" environment and located outside the physical perimeter of the facility via web browser on non-dedicated computer.	High network security needed. Network topology is an issue; control of traffic into PCS network is needed.
UA6	Plant system access with control from mobile device	Access to system with full read-write capability from on-plant location, not physically secured (e.g. plant floor) on mobile device.	
UA7	Remote system access with control from mobile device	Access to system with full read-write capability from location outside "control room" environment and located outside the physical perimeter of the facility on mobile device.	
UA8	Remote system access with view-only from mobile device	Access to system with limited read-only/view capability from location outside "control room" environment and located outside the physical perimeter of the facility on mobile device.	

Category/ Code	Use Case	Description	Security Considerations
UA9	Remote system access with web view from mobile device	Access to web displays of system data with read-only/view capability from location outside "control room" environment and located outside the physical perimeter of the facility via web browser on non-dedicated mobile device.	
UA10	Training environment	System training conducted on production SCADA/Process Control system by 3rd parties.	
UA11	Development environment by SCADA/Process Control staff	System development conducted on production SCADA/Process Control network by SCADA/Process Control personnel.	
UA12	Development environment by external staff or 3rd parties	System development conducted on production SCADA/Process Control network by non-SCADA/Process Control personnel.	

3.3 Cybersecurity Controls

A security control is a measure to support effective cyber defense. Most of the controls in this document are measures designed to reduce risk; they were developed from many industry standards which were correlated, integrated, and enhanced. For example, multiple controls which were similar were merged into a single, more comprehensive control. Some controls are complex and might resemble an administrative program or a computer system. Indeed many software companies develop computer systems to implement controls of greater complexity (e.g., network monitoring tools). Table 3-2 provides a complete list of the cybersecurity controls developed for this document.

Each control was assigned a priority level based on its criticality and potential impact to the security of the utility. Priority levels are defined as follows:

- **Priority 1 Controls** – These controls represent the minimum level of acceptable security for SCADA/PCS. If not already in place, these controls should be implemented immediately.
- **Priority 2 Controls** – These controls should be implemented second because they have the potential to provide a significant and immediate increase in the security of the organization.
- **Priority 3 Controls** – These controls provide additional security against cybersecurity attack of PCS Systems and lay the foundation for implementation of a managed security system. These controls should be implemented as soon as budget allows.
- **Priority 4 Controls** – These controls are more complex and provide protection for more sophisticated attacks (which are less common); they also provide for managed security systems. Many Priority 4 controls are related to policies and procedures; others involve state-of-the-art protection mechanisms. They are important for a complete program as they may offer critical protection against a sophisticated, targeted attack.

Table 3-2
Cybersecurity Controls

AT: Awareness and Training	
AT-1	A security awareness and response program established to ensure staff is aware of security policies and incident response/notification procedures.
AT-2	Security training including Incident response training for employees, contractors and third party users based on job roles.
AT-3	A forensic program established to ensure that evidence is collected/handled in accordance with pertinent laws in case of an incident requiring civil or criminal action.
AU: Audit and Accountability	
AU-1	Audit program established to ensure information systems are compliant with policies and standards and to minimize disruption of operations.
AU-2	Framework of information security policies, procedures, and controls including management's initial and periodic approval established to provide governance, exercise periodic review, dissemination, and coordination of information security activities.
AU-3	Governance framework to disseminate/decentralize decision making while maintaining executive authority and strategic control and ensure that managers follow the security policies and enforce the execution of security procedures within their area of responsibility.
AU-4	Information security responsibilities defined and assigned.
AU-5	Risk based business continuity framework established under the auspices of the executive team to maintain continuity of operations and consistency of policies and plans throughout the organization. Another purpose of the framework is to ensure consistency across plans in terms of priorities, contact data, testing, and maintenance.
AU-6	Policies and procedures established to validate, test, update and audit the business continuity plan throughout the organization.
AU-7	Policies and procedures for system instantiation/deployment established to ensure business continuity.
AU-8	Template for the organization's confidentiality/non-disclosure agreements defined, reviewed, and approved periodically by management.
CM: Configuration Management	
CM-1	Policies for defining business requirements including data validation and message authenticity established to ensure that new/upgraded systems contain appropriate security requirements and controls.
CM-2	Procedure modification tracking program in place to manage and log changes to policies and procedures.
CM-3	Separation of duties implemented for user processes including risk of abuse.
CM-4	Separation of duties implemented for development, production, and testing work.
CM-5	SLAs for all third parties established, including levels of service and change controls.
CM-6	Risk based policies and procedures for change controls, reviews, and audits of SLAs.
CM-7	Monitoring of resources and capabilities with notifications and alarms established to alert management when resources/capabilities fall below a threshold.

IA: Identification and Authentication & Access Control	
IA-1	Access control policies and procedures established including unique user ID for every user, appropriate passwords, privilege accounts, authentication, and management oversight.
IA-2	Access control for the management, monitoring, review, and audit of accounts established including access control, account roles, privilege accounts, password policies and executive oversight.
IA-3	Role based access control system established including policies and procedures.
IA-4	Access control for confidential system documentation established to prevent unauthorized access of trade secrets, program source code, documentation, and passwords (including approved policies and procedures).
IA-5	Access control for diagnostic tools and resources and configuration ports.
IA-6	Access control for networks shared with other parties in accordance with contracts, SLAs and internal policies.
IA-7	Wireless and guest-access framework established for the management, monitoring, review, and audit of wireless and guest access in place.
IA-8	Policies for security of standalone, lost, and misplaced equipment in place.
IA-9	Multifactor authentication system established for critical areas.
IA-10	Policies and procedures for least privilege established to ensure that users only gain access to the authorized services.
IA-11	Workstation and other equipment authentication framework established to secure sensitive access from certain high risk locations.
IA-12	Session controls established to inactivate idle sessions, provide web content filtering, prevent access to malware sites, etc.
IR: Incident Response, Contingency Planning, &Planning	
IR-1	Incident response program established to restore systems and operations based on their criticality and within time constraints and effect recovery in case of a catalogue of disruptive events.
IR-2	A security program established to respond to security incidents monitor, discover, and handle security alerts and technical vulnerabilities, collect and analyze security data, limit the organization's risk profile and ensure that management is aware of changing/emerging risks.
IR-3	A legal/contractual/regulatory framework established to track legal/contractual/regulatory requirements and the efforts to meet them with respect to each important system within the organization. Another purpose of the framework is to ensure compliance of policies and procedures with privacy laws, handling cryptographic products, intellectual property rights, and data retention requirements.
MA: Maintenance	
MA-1	Equipment maintenance/replacement program established to maintain business continuity, availability, and integrity.
MA-2	Maintenance of relationships with authorities, professional associations, interest groups etc., formalized.
MA-3	Off-site equipment maintenance program including risk assessment of outside environmental conditions established.
MP: Media Protection	
MP-1	Storage media management and disposal program established to ensure that any sensitive data/software is used appropriately and is removed prior to media disposal (including approved policies and procedures).
MP-2	Information exit mechanisms in place to prevent data, software leaving premises without authorization or logging.
MP-3	Policies and procedure repository in place to be available to all authorized staff.

PE: Physical and Environmental Protection	
PE-1	Security perimeters, card controlled gates, manned booths, and procedures for entry control.
PE-2	Secure areas protected by entry controls and procedures to ensure that only authorized personnel have access.
PE-3	Physical security and procedures for offices, rooms, and facilities.
PE-4	Physical protection against fire, flood, earthquake, explosion, civil unrest, etc.
PE-5	Physical security and procedures for working in secure areas.
PE-6	Physical security and procedures for mail rooms, loading areas, etc., established. These areas must be isolated from IT/PCS areas.
PE-7	Physical security and procedures against equipment environmental threats and hazards or unauthorized access.
PE-8	Physical/logical protection against power failure of equipment (UPS).
PE-9	Physical/logical protection against access to power and telecommunications cabling established.
PM: Program Management & Security Assessment and Authorization	
PM-1	Asset management program including a repository containing all significant assets of the organization with a responsible party for each, periodic inventories, and audits.
PM-2	Policies and procedures for acceptable use of assets and information approved and implemented.
PM-3	Centralized logging system including policies and procedures to collect, analyze and report to management.
PM-4	SLAs for software and information exchange with internal/external parties in place including interfaces between systems and approved policies and procedures.
PM-5	Data classification policies and procedures for handling and labeling based on confidentiality and criticality approved and implemented.
PS: Personnel Security	
PS-1	Policies and procedures for hiring/terminating processes on employees, contractors, or support companies to include background checks and contract agreements approved and implemented.
PS-2	Defined and approved security roles and responsibilities of all employees, contractors and third party users.
PS-3	A clear desk policy in place including clear papers, media, desktop, and computer screens.
PS-4	Disciplinary process for security violations established.
RA: Risk Assessment	
RA-1	Risk assessment and approval process before granting access to the organization's information systems.
RA-2	Third party agreement process to ensure security on access, processing, communicating, or managing the organization's information or facilities.
SA: System and Services Acquisition	
SA-1	Authorization process established for new systems or changes to existing information processing systems.
SA-2	Change controls of systems development, outsourced development, system modification, and testing established, including acceptance criteria for new systems, monitoring of internal/outsourced development, and control of system upgrades.
SA-3	Change controls of operating systems, network configuration/topology, network security established, including changes to IDS/IPS, traffic control/monitoring, new systems, and system upgrades.
SA-4	Risk based mobility policies and procedures established to protect against inherent risk of mobile computing and communication systems.
SA-5	Periodic review of backup policies and procedures and testing of recovery processes.

SC: System and Communications Protection	
SC-1	Policies and procedures governing cryptography and cryptographic protocols including key/certificate-management established to maximize protection of systems and information.
SC-2	Centralized authentication system or single sign-on established to authorize access from a central system.
SC-3	Policies and procedures established for network segmentation including implementation of DMZs based on type and sensitivity of equipment, user roles, and types of systems established.
SC-4	Intrusion detection, prevention, and recovery systems including approved policies and procedures established to protect against cyber-attacks. System includes repository of fault logging, analysis, and appropriate actions taken.
SC-5	Anomaly based IDS/IPS established including policies and procedures.
SC-6	Network management and monitoring established including deep packet inspection of traffic, QoS, port-level security, and approved policies and procedures.
SC-7	Information exchange protection program in place to protect data in-transit through any communication system including the Internet, email, and text messaging and approved policies and procedures.
SC-8	Routing controls established to provide logical separation of sensitive systems and enforce the organization's access control policy.
SC-9	Process isolation established to provide a manual override “air gap” between highly sensitive systems and regular environments.
SC-10	Program for hardening servers, workstations, routers, and other systems using levels of hardening based on criticality established. Program should include policies and procedures for whitelisting (deny-all, allow by exception).
SC-11	Framework for hardening of mobile code and devices established (including acceptance criteria and approved policies and procedures).
SC-12	Remote access framework including policies and procedures established to provide secure access to telecommuting staff, established for the management, monitoring, review, and audit of remote access to the organization.
SC-13	Testing standards including test data selection, protection, and system verification established to ensure system completeness.
SC-14	Network segregation. Firewalls, deep packet inspection and/or application proxy gateways.
SC-15	Logically separated control network. Minimal or single access points between corporate and control network. Stateful firewall between corporate and control networks filtering on TCP and UDP ports. DMZ networks for data sharing.
SC-16	Defense-in-depth. Multiple layers of security with overlapping functionality.
SC-17	Virtual Local Area Network (VLAN) for logical network segregation.
SC-18	Minimize wireless network coverage.
SC-19	802.1X user authentication on wireless networks.
SC-20	Wireless equipment located on isolated network with minimal or single connection to control network.
SC-21	Unique wireless network identifier (SSID) for control network.
SC-22	Separate Microsoft Windows domain for wireless (if using Windows).
SC-23	Wireless communications links encrypted.
SC-24	Communications links encrypted.
SC-25	Virtual Private Network (VPN) using IPsec, SSL or SSH to encrypt communications from untrusted networks to the control system network.

SI: System and Information Integrity	
SI-1	Electronic commerce infrastructure in place providing integrity, confidentiality and non-repudiation and including adherence to pertinent laws, regulations, policies, procedures, and approval by management.
SI-2	System acceptance standards including data validation (input/output), message authenticity, and system integrity established to detect information corruption during processing.
SI-3	Interactive system for managing password implemented to ensure password strength.
SI-4	Organization-wide clock synchronization system in place.
SI-5	Privileged programs controls established to restrict usage of utility programs that could reset passwords or override controls as well as IT audit tools that can modify or delete audit data.

3.4 Referenced Standards

To provide the user with more detailed information on the steps necessary to implement the recommended cybersecurity controls, specific references to existing NIST, AWWA, and ISA standards are provided. The references provide the specific paragraph or section number in the referenced standard in which the applicable information can be found. Table 3.3 provides a list of the referenced standards.

Table 3-3
List of Standards & Guidance

	Name	Version/Revision Date
ANSI/AWWA G430-14	Security Practices for Operation and Management	November 2014
DHS-CAT	U.S. Department of Homeland Security (DHS) Catalog of Control Systems Security: Recommendations for Standards Developers	April 2011
DHS DID	Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies	October 2009
ISA 62443-1-1	Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models	October 2007
ISA 62443-2-1	Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program	January 2009
ISA 62443-3-3	Security for industrial automation and control systems Part 3-3: System security requirements and security levels	August 2013
ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements	October 2013
ISO/IEC 27003	Information technology — Security techniques — Information security management system implementation guidance	February 2010
ISO/IEC 27005	Information technology — Security techniques — Information security risk management	June 2011
NIST 800-34r1	Contingency Planning Guide for Federal Information Systems	May 2010
NIST 800-53r4	Security and Privacy Controls for Federal Information Systems and Organizations	April 2013
NIST 800-61r2	Computer Security Incident Handling Guide	August 2012
NIST 800-82r2	Guide to Industrial Control Systems (ICS) Security	May 2015
NIST 800-124r1	Guidelines for Managing the Security of Mobile Devices in the Enterprise	June 2013

Appendix A: Cross Reference to NIST Cybersecurity Framework

The following table provides a cross-reference between the Cybersecurity Controls incorporated into the AWWA Cybersecurity Guidance Tool and the Framework Core (Appendix A) included in the Cybersecurity Framework issued by NIST on February 12, 2014.

Function	Category	Sub-Category	Description	AWWA Guidance Control
IDENTIFY	Asset Management	ID.AM-1	Physical devices and systems within the organization are inventoried	PM-2
		ID.AM-2	Software platforms and applications within the organization are inventoried	PM-2
		ID.AM-3	Organizational communication and data flows are mapped	PM-2
		ID.AM-4	External information systems are catalogued	MA-3
		ID.AM-5	Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	PM-5
		ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	PE-4, PS-2
	Business Environment	ID.BE-1	The organization's role in the supply chain is identified and communicated	RA-2, PS-2, CM-5
		ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated	MA-2
		ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated	IR-2
		ID.BE-4	Dependencies and critical functions for delivery of critical services are established	IR-2
		ID.BE-5	Resilience requirements to support delivery of critical services are established	IR-3

Function	Category	Sub-Category	Description	AWWA Guidance Control
IDENTIFY – cont'd	Governance	ID.GV-1	Organizational information security policy is established	IR-2, AU-2
		ID.GV-2	Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	PS-2, AU-4, AU-6
		ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	IR-3
		ID.GV-4	Governance and risk management processes address cybersecurity risks	AU-3, AU-5, CM-6
	Risk Assessment	ID.RA-1	Asset vulnerabilities are identified and documented	AU-5, RA-1, IR-2
		ID.RA-2	Threat and vulnerability information is received from information sharing forums and sources	AU-5, PM-3, IR-2
		ID.RA-3	Threats, both internal and external, are identified and documented	AU-5, RA-1, IR-2
		ID.RA-4	Potential business impacts and likelihoods are identified	AU-5, RA-1, IR-2
		ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	AU-5
		ID.RA-6	Risk responses are identified and prioritized	IR-1
	Risk Management Strategy	ID.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders	IR-2
		ID.RM-2	Organizational risk tolerance is determined and clearly expressed	SA-4
		ID.RM-3	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	SC-4

Function	Category	Sub-Category	Description	AWWA Guidance Control
PROTECT	Access Control	PR.AC-1	Identities and credentials are managed for authorized devices and users	IA-1, RA-1, SC-19
		PR.AC-2	Physical access to assets is managed and protected	PE-1, PE-2, PE-3
		PR.AC-3	Remote access is managed	IA-7, SC-12, SC-18, SC-21, RA-2
		PR.AC-4	Access permissions are managed, incorporating the principles of least privilege and separation of duties	IA-3, SC-22
		PR.AC-5	Network integrity is protected, incorporating network segregation where appropriate	SC-8, SC-9, SC-14, SC-15, SC-16, SC-17, SC-20, SC-25
	Awareness & Training	PR.AT-1	All users are informed and trained	AT-1, AT-2
		PR.AT-2	Privileged users understand roles & responsibilities	AT-1, AT-2
		PR.AT-3	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	AT-2
		PR.AT-4	Senior executives understand roles & responsibilities	AT-1
		PR.AT-5	Physical and information security personnel understand roles & responsibilities	PS-4, AT-1
	Data Security	PR.DS-1	Data-at-rest is protected	PM-5, MP-2
		PR.DS-2	Data-in-transit is protected	PM-4, SC-14, SC-23, SC-24
		PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition	PM-1
		PR.DS-4	Adequate capacity to ensure availability is maintained	MA-1, CM-7
		PR.DS-5	Protections against data leaks are implemented	IA-4
		PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	IR-3

Function	Category	Sub-Category	Description	AWWA Guidance Control
PROTECT – *cont.*		PR.DS-7	The development and testing environment(s) are separate from the production environment	CM-4
	Information Protection Processes and Procedures (IP)	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained	SA-3
		PR.IP-2	A System Development Life Cycle to manage systems is implemented	CM-1, CM-6
		PR.IP-3	Configuration change control processes are in place	SA-3
		PR.IP-4	Backups of information are conducted, maintained, and tested periodically	SA-5
		PR.IP-5	Policy and regulations regarding the physical operating environment for organizational assets are met	PE-4
		PR.IP-6	Data is destroyed according to policy	MP-1
		PR.IP-7	Protection processes are continuously improved	AU-6
		PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties	AU-7
		PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	ANSI/AWWA J100
		PR.IP-10	Response and recovery plans are tested	PS-4
		PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	AT-2
		PR.IP-12	A vulnerability management plan is developed and implemented	AU-5
	Maintenance	PR.MA-1	Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	MA-1
		PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	MA-1

Function	Category	Sub-Category	Description	AWWA Guidance Control
PROTECT – *cont.*	Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	PM-3
		PR.PT-2	Removable media is protected and its use restricted according to policy	MP-1
		PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality [whitelisting]	SC-10, SC-19
		PR.PT-4	Communications and control networks are protected	IA-7
DETECT	Anomalies and Events	DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	Not addressed
		DE.AE-2	Detected events are analyzed to understand attack targets and methods	SC-5
		DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors	Not addressed
		DE.AE-4	Impact of events is determined	PM-3
		DE.AE-5	Incident alert thresholds are established	CM-7
	Security Continuous Monitoring	DE.CM-1	The network is monitored to detect potential cybersecurity events	CM-7
		DE.CM-2	The physical environment is monitored to detect potential cybersecurity events	PE-1, CM-7
		DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	CM-7, SA-5
		DE.CM-4	Malicious code is detected	SC-5
		DE.CM-5	Unauthorized mobile code is detected	SA-4
		DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events	IA-2
		DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	PS-1
		DE.CM-8	Vulnerability scans are performed	IR-2

Function	Category	Sub-Category	Description	AWWA Guidance Control
DETECT – cont'd	Detection Processes	DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability adequate awareness of anomalous events.	PS-2
		DE.DP-2	Detection activities comply with all applicable requirements	IR-3
		DE.DP-3	Detection processes are tested	ANSI/AWWA G430, G440
		DE.DP-4	Event detection information is communicated to appropriate parties	IA-2
		DE.DP-5	Detection processes are continuously improved	SC-4
RESPOND	Response Planning	RS.PL-1	Response plan is executed during or after an event	AT-1
	Communications	RS.CO-1	Personnel know their roles and order of operations when a response is needed	ANSI/AWWA G430, G440, WRF/EPA/AWWA
		RS.CO-2	Events are reported consistent with established criteria	G430
		RS.CO-3	Information is shared consistent with response plans	SC-6
		RS.CO-4	Coordination with stakeholders occurs consistent with response plans	ANSI/AWWA G430, G440, WRF/EPA/AWWA
		RS.CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	MA-2
	Analysis	RS.AN-1	Notifications from detection systems are investigated	SC-5
		RS.AN-2	The impact of the incident is understood	ANSI/AWWA J100
		RS.AN-3	Forensics are performed	AT-3
		RS.AN-4	Incidents are categorized consistent with response plans	AT-3

Function	Category	Sub-Category	Description	AWWA Guidance Control
RESPOND – cont'd	Mitigation	RS.MI-1	Incidents are contained	IR-1
		RS.MI-2	Incidents are mitigated	IR-1
		RS.MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks	IR-2
	Improvements	RS.IM-1	Response plans incorporate lessons learned	ANSI/AWWA G430, G440, WRF/EPA/AWWA
		RS.IM-2	Response strategies are updated	ANSI/AWWA G430, G440, WRF/EPA/AWWA
RECOVER	Recovery Planning	RC.RP-1	Recovery plan is executed during or after an event restoration of systems or assets affected by cybersecurity events.	AU-7
	Improvements	RC.IM-1	Recovery plans incorporate lessons learned	ANSI/AWWA G430, G440, WRF/EPA/AWWA
		RC.IM-2	Recovery strategies are updated	ANSI/AWWA G430, G440, WRF/EPA/AWWA
	Communications	RC.CO-1	Public relations are managed	ANSI/AWWA G430, G440, WRF/EPA/AWWA
		RC.CO-2	Reputation after an event is repaired	ANSI/AWWA G430, G440, WRF/EPA/AWWA
		RC.CO-3	Recovery activities are communicated to internal stakeholders and executive and management teams	ANSI/AWWA G430, G440, WRF/EPA/AWWA

NOTES

American Water Works Association

Dedicated to the World's Most Important Resource™

Government Affairs Office
1300 Eye St. NW, Suite 701W
Washington, DC 20005
T: 202.628.8303
F: 202.628.2846

Dear General Liability Members,

A valuable component of the JPIA's Cyber Liability coverage is access to a vast library of Cyber resources.

Go to **CyberRiskConnect.com and type the access code 10448 to receive** a variety of tools to assist with your mitigation efforts against Cyber Liability risks.

Tools Include:

- **Cyber Liability Library:** latest cyber risk articles and videos, as well as product and policy information from our XL Catlin cyber team.
- **Cyber Training Videos:** A series of educational videos designed to help train clients on their role in keeping sensitive information secure focusing on network security and privacy, incident response planning, the importance of risk assessments and HIPAA.
- **Incident Roadmap:** suggested steps to take following a network or data breach incident.
- **Vendor Partner Resources:** a directory to help clients gain quick access to our recently expanded, pre-qualified network of third-party resources with expertise in pre- and post-breach disciplines, including network vulnerability testing, IT risk assessments, incident response planning, security awareness training, PCI compliance, security incident response planning, data breach tabletops, and more.
- **News Center:** articles and commentary discussing trends, major breach events, security awareness strategies, risk management guidance, and helpful industry links.
- **Risk Manager's Toolbox:** includes a cyber-risk assessment survey, breach notification guides, what-if modeling tools to estimate the cost of a breach, research tools to monitor the type, frequency and severity of incidents occurring in your business sector.

Plus, Sample Policies

- Antivirus and Malware Policy
- Incident Response Plan Policy
- Information Security Policy
- MDM-BYOD Auto-Wipe Waiver
- Mobile Computing Policy
- Personal Device Use (BYOD) Policy
- Physical Security Policy
- Posting and Removal of Online Content
- Sample Information Security Policy Template
- Security Awareness Training and Education Policy
- Security Policy 101 - Essential Policies for Business
- Sensitive Information Handling
- Social Networking Acceptable Use
- Web Site Privacy Policy

Please note the following:

- CyberRiskConnect.com is a private site for only the JPIA. The JPIA is fortunate to have such an array of tools and resources that we ask that you do not share portal access instructions with anyone outside your organization. You are responsible for maintaining the confidentiality of the **Access Code** provided to you.
- Up to five individuals from your district may register and use the portal. Ideal candidates include your company's Risk Manager, Compliance Manager, Privacy Officer, IT Operations Manager or Legal Counsel.
- This portal contains a directory of experienced providers of cyber risk management and breach services. Unless otherwise indicated or approved, payment for services provided by these companies is your responsibility.

If you have questions or comments, please feel free to call Member Services at (916) 786-5742.

Best regards,
Karen

Karen L. Thesing, ARM
ACWA JPIA
Director of Insurance Services
(916) 786-5742 (Office)
(916) 774-7050 x3130 (Direct)
kthesing@acwajpia.com | **acwajpia.com**

eRisk Self-Assessment

powered by NetDiligence

SELF-ASSESSMENT SCORECARD

Company name: eRisk Hub
Invitation sent to: Sample Organization
Submitted on: 11/09/2016 18:12 PM

Quick eRisk Assessment

This is a eRisk Hub sponsored 'fast self-assessment', designed to capture high-level information concerning your company's use of some industry-recognized baseline practices in the areas of IT security.

This eRisk Hub fast self-assessment is based upon a very limited survey (sampling) of network risk factors and industry recognized baseline practices associated with network security and related processes. By offering this NetDiligence nor our alliance partners make any representations about the actual or potential risk exposures associated with the customer, nor do we certify any form of security state or compliance.

Report Card Calculation Methodology

This report card is intended to highlight your organizations' overall score on the Self-Assessment. The total possible score is 100. This report card may indicate areas of improvement for your Network Security and Risk Management Program. For specifics on which areas or questions you scored high and low on, please review the survey and your answers. Negative or "no" responses will indicate the areas for your improvement.

	Section	Summary	Scores		Issues
1	Security Policy A written policy document should be available to all employees responsible for information security.	Ok	Your score	100%	N/A
2	Security Organization To manage information security within the organization, a management framework should be established...	Ok	Your score	75%	N/A
3	Information Asset Classification and Control To maintain appropriate protection of organizational assets and, to ensure that information assets r...	Weak	Your score	0%	N/A
4	Personnel Security To reduce the risks of human error, theft, fraud or misuse of facilities. To ensure that users are a...	Weak	Your score	25%	N/A
5	Physical and Environmental Security To prevent unauthorized access, damage and interference to IT services. To prevent loss, damage or c...	Ok	Your score	80%	N/A
6	Communications and Operations Management To ensure the correct and secure operation of computer and network facilities. To minimize the risk ...	Weak	Your score	49.5%	N/A
7	Access Control To control access to business information. To prevent unauthorized computer access. To prevent unaut...	Ok	Your score	100%	N/A
8	Systems Development and Maintenance To ensure that security is built into IT systems. To ensure that IT projects and support activities ...	Weak	Your score	50%	N/A
9	Business Continuity Management To have plans available to counteract interruptions to business activities, resulting from network a...	Weak	Your score	40%	N/A
10	Compliance Compliance with legal requirements, to mitigate breaches of any statutory, criminal or civil obligat...	Ok	Your score	62.5%	N/A
11	Data Privacy Practices To ensure that there is general awareness of privacy issues surrounding data and information managem...	Ok	Your score	80%	N/A
12	General & Current Events To capture a high level understanding of what your organization is doing to pro-actively address a f...	Ok	Your score	85%	N/A
	Score Average and Total Issue Sections		Your score	62.3%	