Office of Statewide Reporting and Accounting Policy
State of Louisiana
Division of Administration

JOHN BEL EDWARDS
GOVERNOR

JAY DARDENNE
COMMISSIONER OF ADMINISTRATION

December 4, 2019

MEMORANDUM OSRAP 20-10

TO: Fiscal Officers
All State Agencies

FROM: Afranie Adomako, CPA
Director of Management and Finance DOA

SUBJECT: Coding Expenditures and Tracking Lost Revenues Related to Cybersecurity Incident Proclamation no. 173 JBE 2019

Attached is a memorandum from the Commissioner of Administration, Jay Dardenne, requiring all agencies to track all expenditures and lost revenues relating to the declared State of Emergency – Cybersecurity Incident. Please read this memorandum and follow the instructions as indicated.

If you have questions on any part of the memorandum, please contact the control Agencies for the specific functional area in the memorandum.

Office of State Payroll – phone number 225-342-0713
Office of State Procurement – phone number 225-342-8010
Office of Technology Services – phone number 225-342-2677

AA/jbl

Office of the Commissioner
State of Louisiana
Division of Administration

JOHN BEL EDWARDS
GOVERNOR

JAY DARDENNE
COMMISSIONER OF ADMINISTRATION

MEMORANDUM

TO: All Department Secretaries and Undersecretaries

FROM: Jay Dardenne
Commissioner of Administration

DATE: December 4, 2019

SUBJECT: State of Emergency – Cybersecurity Incident – Proclamation No. 173 JBE 2019– Procedures for Coding of Expenditures, Emergency Procurement, Overtime Reimbursement, etc.

With the cybersecurity incident which occurred in several State entities, it is critical to review the required maintenance of emergency-related records and documentation and the required policies and procedures as a result of this event. Please communicate this guidance to your management and staff immediately.

EMERGENCY PROCUREMENT

Emergency procurement and contract procedures can be found in the Division of Administration's emergency procurement guide, which is available on the Office of State Procurement website (http://www.doa.la.gov/osp/agencycenter/publications/emergencyprocurement-08_03_16.pdf), as well as in any executive orders that may be issued by Governor John Bel Edwards.

Any such emergency procurements and/or contracts should emphasize the following:

- Competition, where practical;
- Results-oriented contracts;
- Documentation for audit and reimbursement purposes; and
- Reporting on emergency procurements as soon as practical.

Agencies are encouraged to have employees verify their contact information and to make updates through LEO or their Employee Administration Office. If employees relocate to a temporary address, the mailing address (not permanent residence address) should be changed in LaGov HCM.

OVERTIME

Department and agency heads should review their overtime policies. All such policies should comply with Civil Service Rules, and the FLSA. Departments should have an overtime policy in place guiding the earning and compensation of overtime. Also, departments should have adopted a policy on "Overtime Compensation for Emergency Support Workers" that may supersede their department policy regarding workers who perform duties relative to disaster operations and management.

CODING OF EXPENDITURES AND TRACKING LOST REVENUES

It is critically important that all agencies accurately capture and maintain all records and documentation related to expenditures incurred due to the cybersecurity incident in order for the State of Louisiana to successfully request and receive full reimbursement

Agencies should not, at this time, be concerned with what may or may not qualify for reimbursement; rather, any and all costs related to the cybersecurity incident should be coded to the **"IT02" activity code**. Full and complete documentation and justification of all expenditures will be critical to securing reimbursement. In addition to the impact on expenditure budgets, there will also be revenue impacts related to the cybersecurity incident – decreases to self-generated revenues, lost revenue streams, "savings" due to office closures, etc.

Expenditures

A new "Activity Code" has been established in ISIS to track expenditures related to cybersecurity incident. **If your agency incurs any expenditures related to this event, you must enter "IT02" activity code in the ACTV field or WBS element of any ISIS or SRM ISIS document or the ISIS payment document (PV, PVQ, P1, MW, reclassification of P3, etc.). If you are a LaGov Financial agency, you will enter the Functional Area from the attached list on any LaGov document. If you are a LaGov Financial agency and using Project(s), you will link the Functional Area to the project and it will default on LaGov documents.** If you have already incurred expenditures related to the event that are not coded to this activity code, please prepare a journal voucher to include this activity code so that costs can be captured in an activity report for all state agencies. This procedure is being implemented to track all event related expenditures for the State to be used in future decisions. Invoices for these expenditures should be clearly marked 'Related to the 'Cybersecurity Incident 173 JBE 2019' and, if necessary, should have a brief explanation of why it was necessary to incur the expenditure. It is imperative that these expenditures be properly documented so we can provide substantiations during audit.

Agencies that do NOT utilize the State's ISIS or LaGov systems must develop their own mechanism to capture the cybersecurity incident related expenditures and report this information, upon request, to the Division of Administration (DOA).

Lost Revenues

If your agency has incurred a loss of revenues as a result of cybersecurity incident, you must begin tracking this loss. Estimating will be acceptable and can be accomplished by using the last two years average revenue received during the same period (week/month) last year versus this year. This comparison should be made on a spreadsheet with a line for each type (source) of revenue. It should begin with the last period that had "normal" revenues and then continue with subsequent periods.

Payroll Costs

- WBS Element (formerly referred to as Activity Code): For LaGov ISIS HCM Paid Agencies, the newly created WBS Element "**IT02**" should be utilized if the employee's applicable regular hours worked and/or applicable overtime hours worked are related to activity associated with the cybersecurity incident. LaGov Financial Agencies should follow the same process outlined in the expenditure paragraph for use of Functional Area.
  - Regular Hours Worked:
    - LaGov ISIS HCM Paid Agency Timekeepers should code ZA01 (regular attendance) hours and WBS Element "**IT02**" for regular hours worked. LaGov Financial HCM Paid Agency Timekeepers should code ZA01 (regular attendance) hours and Functional Area or Project as applicable for regular hours worked. Refer to LaGov HCM Help for assistance in entering this data. Note: Agencies should use their discretion in determining which regular hours may qualify for reimbursement.
  - Overtime Hours Worked:
    - LaGov ISIS HCM Paid Agency Timekeepers must code all overtime hours worked related to activity associated with this event to WBS Element "**IT02**". LaGov Financial HCM Paid Agency Timekeepers must code all overtime hours worked related to activity associated with this event to Functional Area or Project. Refer to LaGov HCM Help for assistance in entering this data.

- If retroactive adjustments are necessary, they must be processed through LaGov HCM, not via ISIS journal vouchers.

- **Agencies not paid through LaGov HCM** must develop a mechanism for tracking and reporting this information to the Division of Administration upon request.

Department and agency heads should disseminate this and all future communications from the Division of Administration to all business and administrative functional units (i.e., human resources, payroll, budget, accounting, etc.) within their agencies.

Thank you for your cooperation. Do not hesitate to contact my office if you have any questions or need further information.